(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/24700 A1

(51) International Patent Classification[7]: A61B 5/117, G07C 9/00, G06K 9/00

(21) International Application Number: PCT/US00/27782

(22) International Filing Date: 6 October 2000 (06.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/158,423 7 October 1999 (07.10.1999) US

(71) Applicant *(for all designated States except US)*: **VERIDICOM, INC.** [US/US]; 2040 Martin Avenue, Santa Clara, CA 95050-2702 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **O'GORMAN, Lawrence** [US/US]; 18 Albright Circle, Madison, NJ 07940 (US). **SCHUCKERS, Stephanie** [US/US]; 1282 Forman Drive, Morgantown, WV 26508 (US). **DERAKHSHANI, Reza** [IR/US]; Apt. #K-311, 1056 Van Voorhis Road, Morgantown, WV 26505 (US). **HORNAK, Lawrence** [US/US]; 133 Poplar Drive, BRM, Morgantown, WV 26505 (US). **XIA, Xiongwu** [CN/US]; 31 Scotto Place, South Brunswick, NJ 08810 (US). **D'AMOUR, Michael** [US/US]; 2040 Martin Avenue, Santa Clara, CA 95050 (US).

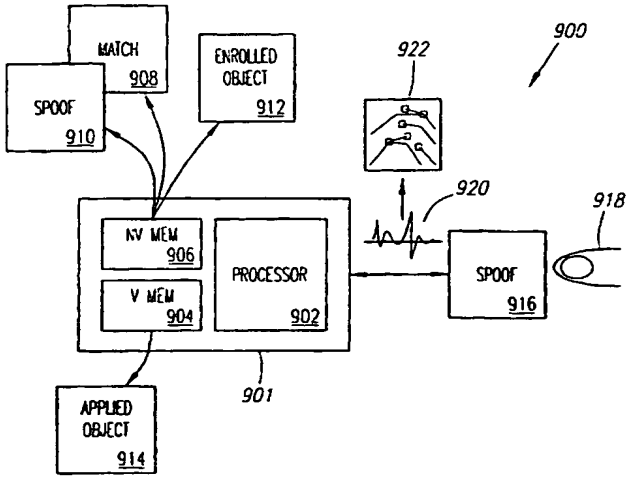
(74) Agents: **HEMMINGER, Steven, D.** et al.; Lyon & Lyon LLP, Suite 4700, 633 West Fifth Street, Los Angeles, CA 90071-2066 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: SPOOF DETECTION FOR BIOMETRIC SENSING SYSTEMS



(57) Abstract: A biometric sensing system and techniques are disclosed for detecting spoofs of a living finger. In accordance with an embodiment of the invention, unique biological and physical characteristics of a finger are captured by a fingerprint sensor over a sequence of images and interpreted from the captured images. The characteristics are extracted from an electrical representation of the finger in what, in the past, was considered "noise" in the electrical representation. According to one embodiment, the system comprises an image capture device configured to sample an applied object and create an electrical representation of the applied object and a spoof detection module configured to analyze the electrical representation of the applied object for relative intensity, density, geometric, or temporal anomalies indicative of a non-living applied object. Methods are disclosed for the same end, the methods including: average intensity, pixel density, rate of warming, ridge uniformity, ridge signal strength, water droplet differential, fingerprint vitality, and inverted spoof techniques.

WO 01/24700 A1

BNSDOCID: <WO 0124700A1 I >

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *With international search report.*

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BNSDOCID: <WO__ 0124700A1 I >

Process this Application in accordance with the
PATENT COOPERATION TREATY

TITLE OF THE INVENTION

Spoof Detection for Biometric Sensing Systems

APPLICANT
Veridicom, Inc.
2040 Martin Ave.
Santa Clara, CA 95050
U.S.A.

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to U.S. Provisional Application Serial No. 60/158,423, filed October 7, 1999, entitled, "Method and Apparatus for Determining a Living Fingerprint on a Fingerprint Sensor," which is incorporated herein by reference in its entirety, and to which priority is claimed.

BACKGROUND

1. Field of the Invention.

The invention relates to biometric sensors, and more particularly to fingerprint sensors and techniques for distinguishing between living and non-living fingers placed on a sensor.

2. Background Information.

Fingerprint identification and authentication systems rely on a user's unique fingerprint to identify whether the user is authorized to access the system. A significant challenge for fingerprint authentication systems is to prevent unauthorized access gained through the use of a spoof, i.e. a fingerprint from a non-living finger. A spoof can include an artificially produced fingerprint (e.g., a molded plastic or rubber 3-dimensional impression of a true fingerprint), a fingerprint from a finger of a dead person, or a fingerprint from a finger severed off of a live person. Each of these spoofs circumvents the fingerprint authentication process, as the spoof can be used separate from its legitimate owner.

One solution to this problem is to require the use of an accompanying password or personal identification number (PIN). All bank cards and most other tokens require both the

BNSDOCID: <WO 0124700A1_1_>

card and a PIN. This combination is a good defense against the spoof attack. Multi-factor authentication is required in many applications not only as a defense against spoofing, but also as an increased level of security.

However, multi-factor authentication has drawbacks. For example, the accounting or card issuing organization faces significant administrative cost in handling the secret codes and the card holders have to memorize the secret codes. In addition to the cost of managing the secret codes, the card issuing organization faces significant cost in handling the cards such as issuing new cards or dealing with lost cards and the card holders have to carry the cards which may be inconvenient to the users in certain situations. Therefore, it is advantageous to capitalize on the inherent benefit of identification through the user's fingerprint, which does not require the user to remember any passwords or to retain any tokens. Accordingly, there is a need to be able to distinguish between living fingers and spoofs, so as to ensure that only authorized persons will be able to access the protected system.

For example, one fairly simple way of illegally accessing an optical fingerprint system is with a photographic copy of a true fingerprint. Older optical fingerprint systems are unable to discriminate between a real fingerprint and a photocopy. To overcome this problem, some optical systems now use frustrated total internal refraction (FTIR), while others employ ultrasound technology. FTIR systems are designed to reflect light from surfaces of the skin directly in contact with the scanner (e.g. fingerprint ridges) and not to reflect light from those surfaces out of contact with the scanner (e.g. fingerprint valleys). Ultrasonic systems such as ones described in U.S. Patent No. 5,587,533 entitled "Surface Feature of Mapping Using High Resolution C-Scan Ultrasonography" of Schneider et al. issued December 24, 1996, direct ultrasonic waves to the object placed on the scanner and monitor the waves that are returned. Both types of optical systems can discriminate between a flat photocopy of a fingerprint and a true fingerprint having 3-dimensional depth. One shortcoming, however, with both of these optical systems is that they cannot distinguish between a living finger and a 3-dimensional finger molded from plastic or rubber, nor a dead from a living finger.

Other approaches are used for non-optical fingerprint authentication systems. For example, some fingerprint capture devices measure the subject's skin resistance and temperature. These measurements can then be compared to normal values for a living finger. If the measurements deviate from normal values, then the fingerprint is identified as a spoof.

BNSDOCID: <WO 0124700A1 I >

The skin resistance and temperature safeguards, however, can easily be circumvented by warming up an artificial or dead finger or by designing an artificial finger with a resistance similar to a true finger.

Still other fingerprint authentication systems utilize other medical measurements to determine whether the fingerprint presented is from a living finger or a spoof. One such system is described in U.S. Patent No. 5,719,950, entitled "Biometric, Personal Authentication System" of Osten et al., issued February 17, 1998, which incorporates biological measurements, such as electrocardiograph signals and blood pressure, in conjunction with a fingerprint scan to determine whether the fingerprint presented originates from a living finger. Disadvantages of these systems include their complexity, large size and high cost. In addition, systems which probe medical signals of a person are highly intrusive.

There is a need, therefore, for an improved method for distinguishing a living finger from a spoof. In particular, the method should accurately discern between the two without being overly intrusive. The method also should not significantly increase the size or cost of the system.

SUMMARY OF THE INVENTION

A method and apparatus for employing spoof detection for a biometric sensing device is provided. The invention employs a number of computer implemented techniques designed to distinguish between a living and a non-living biometric, particularly a fingerprint. Anomalies of an electrical representation of a fingerprint, captured from the biometric sensing device, are analyzed using any number of steps designed to detect certain characteristics that are difficult to spoof and largely unique to a living finger.

According to one embodiment, a solid state fingerprint sensor is employed. One such solid state sensor is a capacitive sensor that captures fingerprints by electrical means. Depth is determined by electric field strength, which is inversely proportional to distance. Because capacitive fingerprint sensors require a three-dimensional object, they do not accept a photographic copy of a true fingerprint. In addition, in order for these sensors to capture a fingerprint, the finger or object presented to the sensor must have electrostatic characteristics similar to the skin on a living finger. This will eliminate fingerprints from plastic or rubber molded fingers, as these materials are non-conductive.

The method further relies on additional characteristics of living fingers that cannot be easily replicated by an artificial, dead or severed finger. For example, living skin has the

BNSDOCID: <WO_ 0124700A1_I_>

functions of excretion of substances through sweat glands and absorption of lipid-soluble substances. Sweat glands include pores which are small openings of the sweat ducts in the skin surface. Pore patterns are unique and they do not disappear, move, or spontaneously change over time. The sweat glands also produce unique characteristics of a living finger. For example, a living finger being a heat source, which warms up the sensor after it is placed on a fingerprint sensor; a living finger perspires; and the skin of a living finger is hydrophilic. Accordingly, the invention analyzes the electrical representation of the fingerprint for characteristics such as intensity or density, as well as, in some embodiments, spatial, geometric, and/or temporal anomalies largely inconsistent with a living finger.

The above characteristics may be observed over a series of captured images. With an increase in temperature, a living finger perspires. Therefore, areas surrounding pores in the finger produce stronger signals. Because the skin of a living finger is hydrophilic, it absorbs liquid. Thus, even with perspiration, a living finger placed on the sensor is capable of generating an image that exhibits good differentiation between the ridges and valleys of the finger.

According to one embodiment, the invention is a biometric sensing system including an image capture device configured to sample an applied object and create an electrical representation of the applied object and a spoof detection module configured to analyze the electrical representation of the applied object for relative intensity, density, geometric, or temporal anomalies indicative of a non-living applied object. Various methods for the spoof detection module are described below.

In one embodiment, the method includes capturing a sequence of images of the applied object from the sensor and calculating an average intensity for each image. In one embodiment, the average intensity is calculated based on the entire image. In another embodiment, the average intensity is calculated based on a portion of the image. In still another embodiment, the average intensity is ON-pixel normalized, meaning that only pixels having a signal exceeding a predetermined threshold value that indicates a fingerprint ridge are used for this calculation. The method further includes successively comparing the average intensities of the sequence of images to determine whether they vary beyond a predetermined threshold amount. If the averages vary beyond the threshold amount, then the system accepts the image as coming from a live person. If the averages do not vary beyond the threshold amount, then the system acquires an additional image of the applied object and calculates the average intensity for that image.

BNSDOCID: <WO_ 0124700A1_I_>

The average intensity of the additional image is compared with the prior averages for the sequence of images to determine whether the averages vary beyond the threshold amount. If the averages still do not vary beyond the threshold amount, then the system repeats the steps of acquiring another image, calculating the average intensity for that image, and comparing that average with the previous ones, until the maximum number of images have been captured. At that point, the system rejects the applied object as being a spoof, rather than a living finger.

In another embodiment, the density of the ON-pixels is calculated over a sequence of images instead of average intensity. In one embodiment, maximum and minimum pixel values for an image (either the entire image or a selected portion of an image) are determined. A mid-value is then determined. A pixel with a value greater than the mid-value is considered to be an ON-pixel. The number of ON-pixels over the number of total pixels (in either the entire image or a selected portion of an image) is the density of an image. The density of each image in the sequence is successively compared with the density of the previous image. An increase in density over the sequence of images exceeding a predetermined threshold amount indicates that the object is from a live person. Otherwise, the object is a spoof.

In still another embodiment, the average intensity is calculated separately for the middle fingerprint portion and the outer fingerprint portion for each image in the sequence of images. Each average intensity of the middle fingerprint portion is successively compared with the average intensity of the middle fingerprint portion of a previously captured image. Likewise, each average intensity of the outer fingerprint portion is successively compared with the average intensity of the outer fingerprint portion of a previously captured image. If the average intensity for the outer fingerprint portion increases faster than the average intensity for the middle fingerprint portion, then the fingerprint is determined to be coming from a spoof. Calculating and comparing the rate of increase for the middle fingerprint portion and the outer fingerprint portion protects the system from falsely accepting an artificially warmed spoof. This is because the middle fingerprint portion warms up faster than the outer fingerprint portion for a living finger while the outer fingerprint portion warms up faster than the middle fingerprint portion for an artificially warmed spoof.

In an alternative embodiment, the density of the middle fingerprint portion and the density for the outer fingerprint portion are calculated and successively compared. If the

BNSDOCID: <WO 0124700A1 I >

density for the middle fingerprint portion increases at a rate that is faster than the outer fingerprint portion, then the image is coming from a living finger.

In one embodiment, the rate of warming for the sequence of captured images is calculated and compared with the rate of warming of the finger during enrollment or during a previous successful verification. The rate of warming, in one embodiment, is calculated using average intensity. In an alternative embodiment, the rate of warming is calculated using density. Comparing the rate of warming for an applied object and a previously determined rate of warming prevents false acceptance of an artificially warmed spoof because the rate of warming of a living finger differs from the rate of warming of a spoof.

In one embodiment, the changes in intensity along the ridges are measured over a sequence of images. If the intensity along ridges increases in a spatially non-uniform way, then the image is accepted as coming from a live person because a spatially non-uniform increase in intensity along the ridges indicates pores emanating sweat which is an indicator of a living finger.

In an alternative embodiment, the nonuniformly increasing intensity is measured along the contours of ridges to obtain a linear sequence of intensity values. The linear sequence depends on the intensity along the ridge. For example, the typical ridge comprises pixels having intensities that increase as they get closer to a pore and decrease as they get further from the pore. Thus, the signal of the contour is typically sinusoidal and has a particular frequency. Since a spoof has no pores, the signal of the contour does not have a frequency related to pore-to-pore frequency. In other words, the signal from a spoof is not sinusoidal. In one embodiment, the intensity periodicity and nonuniformity of the pore-to-pore frequency content in a specific window are measured by Fourier transform.

In one embodiment, the signals for the ridges of the sequence of images are compared. If there are no changes in the signals along a ridge, then the system determines whether the signals are at a maximum. In addition to no signal change along a ridge, a maximum signal strength can indicate that a living finger that is wetted, a living finger that is saturated due to perspiration, or a spoof saturated with moisture. In one circumstance, the system accepts the image as coming from a living finger. In another embodiment, the system notifies the user to wipe excess moisture off the applied object or the sensor and to try again.

In one embodiment, water droplets are located and their sizes measured for each image in the sequence of images. In one embodiment, a water droplet image is a group of pixels having a width exceeding the width of a ridge (note that the ridge is narrow and long

BNSDOCID: <WO_ 0124700A1 I >

while the water droplet is fat and short). The sizes of the water droplets are successively compared. The same or decreasing sizes can indicate that the object is a wetted spoof, or the object is a living finger with over-accumulation of surface moisture. The system rejects the fingerprint. Again, the system can instruct the user to wipe off excessive moisture from the applied object or sensor and try again.

In one embodiment, matching minutiae are further compared with respect to their minutia type, that is, endpoint or bifurcation. The ratio of mismatches of minutia type to the overall minutia matches is compared against a threshold amount. If the ratio exceeds the threshold value, then the sensed fingerprint is rejected as a spoof.

In still another embodiment, the same finger is to be disposed over on the sensor multiple times -- e.g. twice. A sequence of images are captured each time. The sequences of images are then compared. For a true finger, the first image in the second sequence exhibits characteristics closer to the last image in the first sequence while for a spoof, the first image in the second sequence exhibits characteristics closer to the first image in the first sequence.

In another embodiment, two-dimensional captured images are mapped into one-dimensional signals. Static (e.g. from one fingerprint image) and dynamic (e.g. temporal change of perspiration pattern of the skin) measures are then extracted and used for classification. The static and dynamic measures can include those detectable within the same signal derived from one fingerprint image and those observed in temporal transition from one signal to the next such as temporal changes over multiple image signals, respectively. The static measure can be used to detect variations in gray level due to darkening around the pores and the dynamic measure can be used to detect the changes caused by perspiration over time. These measurements are quantified to produce a sweating pattern.

In one embodiment, the calculated parameters, for example, the energy inside normal pore frequency window, total swing ratio, minimum/maximum growth ratio, last-first fingerprint signal difference mean and percentage change of standard deviations, are fed into a neural network. According to one instance, if the output of the neural network is in a predetermined range, then the applied object passes as coming from a living finger. In another instance, the predetermined range is positive. If the output of the neural network is in a second predetermined range, then it is determined whether a predetermined number of trials have been met. In one embodiment, the second predetermined range is negative. If the number of trials is less than a predetermined number of maximum trials, then the system prompts the user to wipe the applied object. The system then captures another sequence of

BNSDOCID: <WO__ 0124700A1_I_>

images. The system repeats the process until the predetermined number of maximum trials has been met, at which time the system rejects the fingerprint as coming from a spoof.

The methods are typically embodied in computer software product executed and/or interpreted by one or more processors. The processor(s) can be part of a network system, a stand-alone computer, an automated teller machine, a wireless telephone, or a smart card, for instance.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1, which comprises FIG. 1A and FIG. 1B arranged in a manner shown in the key to FIG. 1, is a flowchart of a method for distinguishing between a living finger and a spoof by calculating average intensities of a sequence of images.

FIG. 2 shows a block diagram of a fingerprint system.

FIG. 3, which comprises FIG. 3A and FIG. 3B arranged in a manner shown in the key to FIG. 3, is a flowchart of a method for distinguishing between a living finger and a spoof by calculating density of a sequence of images.

FIG. 4 is a flowchart of a method for distinguishing between a living finger and a spoof by calculating the average intensity change along a ridge.

FIG. 5 is a flowchart of a method for distinguishing between a living finger and a spoof by determining whether the average intensity changes along the ridges and whether the average intensities at the ridges are at a maximum value.

FIG. 6 is a flowchart of a method for distinguishing between a living finger and a spoof by comparing the size of water droplets on a sequence of images.

FIG. 7, which comprises FIG. 7A and FIG. 7B arranged in a manner shown in the key to FIG. 7, is a flowchart of a method for distinguishing between a living finger and a spoof based on perspiration characteristics.

FIG. 8 is a flowchart depicting a method for distinguishing between a living finger and an inverted spoof of the living finger.

FIG. 9A is a block diagram of an exemplary biometric sensing system.

FIG. 9B is a block diagram of a capacitive fingerprint sensor.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In accordance with the invention, computer implemented methods and associated apparatuses for distinguishing a living finger from a spoof are provided. A living finger, as

BNSDOCID: <WO_ 0124700A1 I >

opposed to a fake or a dead finger, exhibits vitality, meaning that it has blood flow, perspiration, neuroactivity and other biological functions. For example, living skin has the functions of excretion of substances through sweat glands and absorption of lipid-soluble substances. Each square inch of skin includes approximately 600 sweat glands. Sweat glands include pores, which are small openings of the sweat ducts in the skin surface. Pore patterns are unique and they do not disappear, move, or spontaneously change over time. Typically, pore-to-pore distance is approximately 0.5 mm, or there are approximately 20.8 pores per centimeter (cm) on the ridge. The sweat glands produce some unique biological effects such as the production of heat and moisture (perspiration), as well as the absorption of moisture.

A living finger is a heat source. Therefore, after a living finger is placed on a fingerprint sensor, the finger will warm the sensor. This increase in sensor temperature over a sequence of images can indicate a living finger. In one embodiment, the temperature change is measured directly such as with a heat sensor or the equivalent. In another embodiment, the temperature change is measured indirectly. For instance, increasing temperature causes increasing surface moisture on the finger (due to perspiration).

A living finger perspires. Because moisture is conductive, conductivity increases with increasing moisture. Therefore, if measured by a resistive sensor, then resistance decreases can be observed and, if measured by a capacitive sensor, then capacitance increases can be observed. In addition to an increase/decrease in signal strength, the area of the increased/decreased signal strength expands as perspiration emanates from pore locations along the ridges.

Skin on a living finger is hydrophilic, that is, it absorbs water and other liquids applied at the surface of the skin. Hence, moistures are evenly distributed over the finger and when a living finger is wetted, either with liquid or from perspiration, a quality image having good differentiation between ridges and valleys of the finger may still be generated. This is opposed to a wetted spoof, which can be hydrophobic and tends to pool the moisture in the valleys, thereby yielding little or no ridge to valley differentiation.

Moreover, the texture of the skin has particular characteristics where transitions between ridges and valleys, i.e., at endpoints and bifurcations, occur.

In accordance with an embodiment of the invention, these unique biological and physical characteristics are captured by a fingerprint sensor over a sequence of images and interpreted from the captured images. They are not necessarily measured directly by

BNSDOCID: <WO__0124700A1 I >

biosensors, but rather extracted from the electrical representation of the finger in what may have, in the past, been considered "noise" in the electrical representation.

SYSTEM OVERVIEW

FIGS. 9A-B are block diagrams of an embodiment of the biometric sensing system. Biometric sensing system 900 comprises a processing unit 901 and a sensor 916. The two are communicatively coupled, for instance, by a serial port, or a common bus. The processing unit 901 comprises a processor 902, such as a Motorola 6800 or 68000 series microprocessor. Further included in the processing unit is volatile memory 904 (e.g. RAM), in which temporary variables and executed program code can reside, and a non-volatile memory 906 (e.g., ROM, EPROM, EEPROM, or FLASH), in which persistent program code (to be later executed, for instance) and data reside.

According to one embodiment, the non-volatile memory 906 holds a minutia matching module 908, which is computer program code for finding matches between minutia of the electrical representation of an applied object 914 (a finger 918). An exemplary matching module is described in U.S. Patent Application Serial No. 09/354,929, filed November 17, 1999, entitled "Method and System for Fingerprint Template Matching," which is incorporated herein by reference in its entirety. Another matching module can include the techniques embodiment in U.S. Patent Application Serial No. 09/501,355, filed February 9, 2000, entitled "Biometric False Accept Detection," which is also incorporated herein by reference in its entirety.

An enrolled object 912, which was previously captured and verified, is also stored in non-volatile memory 906. One embodiment of a data structure that can be used to hold information representative of the enrolled object is described in PCT International Application Serial No. PCT/US00/18714, filed July 7, 2000, entitled "Multi-Dimensional Fingerprint Minutia Data Constellation," which is incorporated herein by reference in its entirety.

Furthermore, the non-volatile memory 906 includes and spoof detection module, which can also be computer program code, implementing the methods described in detail below, which distinguishes between a living applied object and a non-living applied object. (It is appreciated that the particular memory or component arrangement can vary -- for instance, the various modules and memories might not all be physically resident in a single

BNSDOCID: <WO__0124700A1_I_>

location, but can be distributed and "logically" arranged as depicted in FIG. 9A. The figure and description is intended to capture this logically arrangement.)

While the program code is ultimately embodied in a system as depicted, for instance, in FIG. 9A, the program code can be sequences of instructions for causing a processor (or distributed processors) to perform the functionalities described above (and more particularly below). The program code, or "software product", can be stored in a tangible medium, such as a CD-ROM, floppy disk, or a computer memory, for instance a shared memory or shared disk on a networked computer system. Further still, the software product can be embodied in downloadable, and perhaps compressed and encrypted, computer data files that are later loaded and executed (or interpreted) by a general purpose computer or an image capture device. According to one embodiment, the invention is completely represented by the spoof detection module software alone -- and can be sold as a stand-alone product augmenting or improving an existing image capture device and/or biometric matching module.

The sensor 916 is preferably a capacitive fingerprint sensor. It is further described with reference to FIG. 9B, to which we now turn.

FIG. 9B shows a diagram of a fingerprint imaging device 932. In normal operation, the fingerprint imaging device 932 uses techniques derived from Coulombs law to determine the location of ridges and valleys in a fingerprint surface 938. By modeling each sensing element 936 in the sensor chip 916 as one plate in a capacitor, the finger surface 938 (that is, the ridges and valleys) being the second plate in the capacitor, it is possible to measure a relative distance between the ridges and valleys to construct an electrical representation of the fingerprint. According to one embodiment, a passivation layer 924 is disposed over the sensing elements 936 to form the capacitor at the ridges.

Turning back to FIG. 9A, when the sensor 916 detects an applied object 918 and captures an image, the individual sensing elements 936 create an electrical representation 920 of the surface 938 of the skin. In an abstract form, the electrical representation may be modeled as the fingerprint 922, wherein particular minutiae are highlighted by boxes only for the purpose of illustration. What is captured, however, is more than simply data representative of ridges and valleys in a fingerprint; anomalies, or "noise" (as is mentioned above) in the image will inevitably occur. These anomalies are discarded by prior systems, but here they are used to computationally analyze the electrical representation 920 for indicia of a living finger.

BNSDOCID: <WO 0124700A1 I >

FIG. 2 is a block diagram of an alternative embodiment of a fingerprint system 5 for implementing the processes described below. Fingerprint system 5, in one embodiment, includes a fingerprint sensor 10 coupled to a processor 6 via a communication line 9. Fingerprint sensor 10 is for capturing fingerprint images from an applied object (e.g. finger 16) and is described in detail below. Processor 6 may be any processor capable of executing a software program. For example, processor 6 may be a central processing unit (CPU) of a conventional personal computer having a monitor 7, keyboard 8 and other peripheral devices (not shown) such as a mouse, biomedical measurement devices, and/or other biometric devices coupled thereto. Communication line 9 can be a serial communication path, such as a universal serial bus, between a serial interface of processor 6 and fingerprint sensor 10.

AVERAGE INTENSITY TECHNIQUE

FIG. 1 is a flowchart of a process of determining whether a fingerprint is coming from a living finger by calculating and comparing the average intensity of each image in a sequence of captured images.

The process of determining whether a fingerprint is coming from a living finger starts in box 102. An image is captured from an applied object by a fingerprint sensor in step 104. The image can be captured using, for example, a solid state fingerprint sensor, such as a capacitive sensor described in U.S. Patent Nos. 6,016,355, entitled "Capacitive Fingerprint Sensor," and 6,049,620, entitled "Capacitive Fingerprint Sensor with Adjustable Gain," and U.S. Patent Application Serial No. 09/354,386, filed July 14, 1999, entitled "A method of Constructing an Ultra-Rugged Biometric I.C. Sensor," and PCT International Application Serial No. PCT/US00/19227, filed July 13, 2000, entitled "Ultra-Rugged I.C. Sensor and Method for Making the Same," which are all incorporated herein by reference in their entirety. Capacitive sensors, such as those described in the above-mentioned references are manufactured using conventional CMOS silicon fabrication technology and include an array of pixels, each pixel comprising a capacitive sensing element. An exemplary sensor has an array of 300x300 pixels. In another embodiment, the image can be captured by a radio frequency based sensor, the radio frequency based sensor detecting surface texture or depth differentials between one or more layers of skin. In still another embodiment, the sensor can be a thermal sensor. In yet another embodiment, the sensor can be a swipe type sensor. (It is noted that these sensor embodiments can be employed in any of the techniques described below.)

BNSDOCID: <WO_ 0124700A1 I >

Because capacitive fingerprint sensors require a three-dimensional object, they do not accept a two-dimensional photographic copy of a fingerprint. In addition, in order for these sensors to capture a fingerprint, the finger or object presented to the sensor must have electrostatic characteristics similar to the skin on a living finger. In other words, the object must be conductive. By requiring such electrostatic characteristics, fingerprints from plastic or rubber molded fingers can be eliminated, as these materials are non-conductive. Of course, other types of fingerprint sensors, e.g., optical sensors and pressures sensors, can be used as well.

Typically, the system uses a raw fingerprint image captured by the sensor to perform the spoof detection methods described herein. It is typically the case that the types of properties described herein, when electrically reproduced by the sensor, are found not, strictly speaking, found in ridge and valley data reproduced by the sensor. Rather, the properties are found in anomalies in the expected (perfect) fingerprint image and/or in other "non-linearities" or disturbances in the image. Thus, it may be undesirable in most, but not all, circumstances to process the raw fingerprint image to reduce the noise and enhance the raw image.

While some tests described below may benefit from such image processing, others may not. (Of course, alternatively, in some embodiments, once it has been determined the sampled image is a living fingerprint (and not a spoof), it may then be desirable to further process the raw data.) So, by way of example, image processing and/or filtering techniques such as those described in U.S. Patent No. 6,049,620, incorporated herein by reference above, U.S. Patent Application Serial Nos. 08/971,455, filed November 17, 1997, entitled "Automatic Adjustment Processing for Sensor Devices," Serial No. 09/300,087, filed April 26, 1999, entitled "Method for Imaging Fingerprints and Concealing Latent Fingerprints," and Serial No. 09/560,702, filed April 27, 2000, entitled "Automatic Gain Amplifier," which are each incorporated herein by reference in their entirety, can be employed.

Measurement for each pixel in the image can be translated into an analog signal representing the intensity of the pixel. In one embodiment, the value of the intensity is represented by a grayscale of 0 to 255 or 8 bits, 0 being the lightest (white, no signal) and 255 being the darkest (black, strong signal).

In general, an image generated from the conductivity measurements of a capacitive fingerprint sensor exhibits darker and lighter areas. These areas represent various levels of conductivity measured at the capacitors. As the finger, which acts as one plate of the

BNSDOCID: <WO _ 0124700A1 I >

capacitor, becomes more conductive from moisture within the skin and on the skin surface (from perspiration), the image gets stronger, meaning that the intensity at each pixel increases. Furthermore, the darker intensity emanates from pore locations along the ridges as sweat is generated at these pore locations. As a result, image quality changes over time and these changes are secondary effects of the above-described biological characteristics. Hence, a sequence of images that exhibits an increase in image intensity may be deemed to be coming from a living finger.

An average intensity is calculated for the captured image in step 106. In one embodiment, the average intensity is ON-pixel normalized. That is, the average intensity of a captured image is an average of the intensities of the pixels that exhibit signal strengths that are greater than an ON-pixel threshold amount. The ON-pixel threshold is important in picture processing for extracting objects from their background and in this case, extracting ridges and valleys from a fingerprint. There are techniques that are known in the image processing arts for selecting an adequate threshold of gray level. One such technique example is described by N. Otsu in "A Threshold Selection Method From Gray-Level Histograms," IEEE Trans. Systems, Man, and Cybernetics, Vol. SMC-9, No. 1, Jan. 1979, pp. 62-66, which is incorporated herein by reference. In one embodiment, the ON-pixel threshold is 10. Thus, a pixel having a signal strength of 10 (e.g. on a scale of 0 to 255) is considered to be an ON-pixel (e.g. a ridge pixel).

In one embodiment, the average intensity is calculated for the full image, which can consist of the entire sensor area, e.g. 300x300 pixels. In another embodiment, the average intensity is calculated based on a portion of the captured image, for example, approximately 1/3 to approximately 2/3 of the central portion of the captured image. Calculation based on a portion of the captured image can reduce computational complexity without losing significant data because the central portion of the image typically contains the majority of the fingerprint image data.

The system then determines whether the captured image is a first image (step 108). If the captured image is a first captured image, then the capture device waits for a predetermined period of time in step 109, prior to capturing another fingerprint image (step 104). The predetermined time period is the actual capture rate, or the time between the capturing of two images. In one embodiment, actual capture rate is approximately 0.2 seconds. In general, actual capture rate depends on the capture device's capture rate (which

BNSDOCID: <WO_ 0124700A1 I >

may be limited due to a particular physical or electrical configuration). The actual capture rate should give sufficient time for a detectable change in the level of the average intensity.

If the currently captured image is not the first image (step 108), then a delta average intensity is calculated from the average intensities of the currently captured image and the previous captured image in step 110. The delta average intensity between each two successively captured images is calculated by subtracting the average intensity of the previous captured image from the average intensity of the currently captured image.

In the embodiment shown in FIG. 1, the delta average intensity is calculated as each image is captured, on an image-by-image basis. In an alternative embodiment, the delta average intensity between each two successively captured images is calculated after a predetermined minimum number of images have been captured.

The system then determines whether the delta average intensity is positive in step 112. A counter that records the number of positive delta average intensities is incremented by one in step 114 if the delta average intensity is positive. The system then determines whether N1 images have been captured in step 116. Similarly, if the delta average intensity is not positive (step 112), then the system does not increment the counter but determines whether N1 images have been captured in step 116.

The value of number N1 depends on the rate of capture of the fingerprint sensor. According to one embodiment, using a capacitive fingerprint sensor, the minimum time for a sufficient change over the sequence of captured images is approximately 1.2 seconds. In this embodiment, at a capture rate of 0.2 seconds, six images are captured prior to any determination of whether the fingerprint is coming from a living finger. Similarly, if the capture device has a capture rate of, for example, 0.02 seconds per image, then a minimum of 60 images are captured prior to any determination.

If N1 images have not been captured (step 116), then an additional fingerprint image is captured in step 104 after a time delay (step 109). Steps 104 through steps 116 are repeated until N1 images have been captured.

After N1 images have been captured, an average delta average intensity is calculated in step 118. The average delta average intensity is calculated as (average of delta average intensities / average of average intensities). For example, for six average intensities (from six captured images) of 80, 90, 100, 110, 120 and 130, the average delta average intensity is calculated as:

$$[(10+10+10+10+10) / 5] / [(80+90+100+110+120+130) / 6] \times 100 \cong 9.5\%.$$

BNSDOCID: <WO__ 0124700A1_I >

The system then determines whether the average intensity is increasing monotonically for the sequence of captured images (step 120). Monotonically increasing average intensity indicates that the applied object is warming up which is an indication of a living finger. A monotonically increasing average intensity is characterized by, for instance, 80% of the captured images having a positive delta average intensity.

An example is illustrative. If six images are captured, the same as in the above example, then the five delta average intensities are +10, +10, +10, +10, and +10. Since 100% of the images exhibit an increase in average intensity, the average intensity increases monotonically.

If the average intensity increases monotonically (step 120), then the system determines whether the average delta intensity is greater than a predetermined threshold amount (step 122). In one embodiment, the predetermined threshold is 10%. This value is selected based on experimentation. If the average delta intensity is greater than the predetermined threshold amount (step 122), then the image is accepted as coming from a living finger (step 124) and the process ends in step 126. All counters are reset at step 126. It is noted that steps 120 and 122 may be reversed in sequence or executed in parallel.

After N1 images have been captured, if the average intensity does not increase monotonically (step 120), or the average delta average intensity does not exceed the predetermined threshold amount (step 122), then a decision cannot be made as to whether the captured image is coming from a living finger or a spoof. When the decision cannot be made in the minimum time, e.g. 1.2 seconds for 6 images captured at a rate of 0.2 seconds, it is determined whether N2 images have been captured (step 128). N2 is the maximum number of images captured for the system to make a decision. If N2 images have not been captured (step 128), then an additional image is captured (step 104) after the time delay (step 109) until N2 images have been captured or until the system determines that the image is coming from a living finger. In one embodiment, the value of N2 is 15 (or the capture time is 3 seconds).

The average intensity of the additional image is calculated in step 106. The delta average intensity is calculated (step 110). The average delta average intensity is calculated (step 118). The system then determines whether the average intensity increases monotonically (step 120) and whether the average delta average intensity is greater than the threshold amount (step 122) as described above. If the average intensity increases

BNSDOCID: <WO_ 0124700A1_I >

monotonically (step 120) and the average delta intensity is above a predetermined threshold amount (step 122), then the image is accepted as coming from a living finger (step 124).

If, however, the average intensity is not increasing monotonically or the average delta intensity is not greater the threshold amount and N2 images have been captured, then the image is rejected as coming from a spoof (step 130) and the process ends in step 126. In a static imaging environment, i.e. an environment where the applied object does not move relative to the sensor for image capture purposes, it is noted that the applied object, e.g. the finger, should remain on the fingerprint sensor until a decision is made. For example, the applied object must remain relatively stationary on the fingerprint sensor for a minimum of 1.2 seconds.

It is noted that in the embodiment above (FIG. 1), uniform sensor devices should be employed because different devices give different ranges of intensities. Since intensity ranges vary with different devices, it is difficult to use a fixed threshold while obtaining good or uniform results for all the devices. In addition, different fingers also give different ranges of intensities. Accordingly, the lack in uniformity causes it to be even more difficult to use a fixed threshold. Hence, where uniformity of the sensor is a concern, software and/or hardware based normalization may need to be performed on the sampled image(s) so that a different threshold does not need to be calculated for different people or different devices. Filtering and image processing techniques, such as those mentioned above for instance U.S. Patent Application Serial No. 09/560,702, filed April 27, 2000, as well as those discussed below, can be employed to achieve such a normalization.

PIXEL DENSITY TECHNIQUE

A more robust way of testing vitality is to use the density of ON-pixels along a ridge. Density is a measurement of the number of ON-pixels in a certain area, the certain area being the normalization factor. Because increased moisture within and on the surface of the skin increases the signals and that as the finger is warming up the sensor, the moisture increases, in particular, along the ridges. Hence, the ridge area is used in measuring the density of ON-pixels.

FIG. 3 shows a flowchart for determining whether a fingerprint is coming from a living finger by calculating the density of ON-pixels in a predetermined area. The process starts in step 150. A fingerprint image is captured in step 152. A portion of the captured image is selected in step 154. In one embodiment, a central portion of an image is selected.

BNSDOCID: <WO 0124700A1 >

For example, approximately 1/3 to approximately 2/3 of the central portion of the image is selected. In step 156, a maximum intensity value and a minimum intensity value for the pixels in the selected area are established. A mid-value between the maximum intensity value and the minimum intensity value is then determined in step 158. A pixel in the selected portion having an intensity value above the mid-value indicates an ON-pixel, or a ridge pixel (step 160). The ON-pixels in the selected portion are counted in step 162. Also in step 162, the density of the full image, or a portion thereof, is calculated by dividing the number of the ON-pixels into the total pixels in the selected portion.

The system then determines whether the captured image is the first image captured (step 164). If the captured image is the first image captured, then another fingerprint image is captured after a time delay (i.e. at a predetermined capture rate) in step 152. If the captured image is not the first image captured, then the change in density between the current captured image and the previous captured image is calculated in step 166.

The system then determines whether N3 images have been captured in step 168. Parameter N3 is the minimum number of images required prior to determining whether an image is coming from a living finger. If N3 images have not been captured, then another image is captured after a time delay (step 152). If N3 images have been captured, then the system determines whether the density increases monotonically in step 170. Similar to that described above, a counter counts the number of positive delta densities. If the number of positive delta densities exceeds a predetermined percentage, then the density of the sequence of images increase monotonically.

If the density does not increase monotonically, then the system checks whether N4 images have been captured in step 180. N4 is the maximum number of images captured for determining whether an image is coming from a living finger, similar to N2 described above. If the maximum number of images have not been captured, then another image is captured in step 152 after a time delay. If the maximum number of images have been captured, then the system rejects the image as coming from a spoof (step 182).

If the density increases monotonically, then the system calculates the average delta density (Step 172). Specifically, the delta densities are averaged and divided by the averaged density. If the average delta density exceeds a predetermined threshold amount (step 174), then the image is accepted as coming from a living finger (step 176) and the process ends in step 178. In one embodiment, the threshold amount is 0.35%.

BNSDOCID: <WO_ 0124700A1 I >

If, however, the average delta density does not exceed the threshold, then it is determined whether N4 images have been captured (step 180). If less than N4 images have been captured, then an additional fingerprint image is capture in step 152 after a time delay. It is noted that all counters are reset in end step 178.

In one embodiment, to protect the system from falsely accepting an artificially warmed spoof, e.g. a spoof that is warmed by a hair blower, image characteristics are measured at different portions of the fingerprint. For instance, measurements can be taken from the middle of the fingerprint (middle fingerprint portion) and the outer peripheral of the fingerprint (outer fingerprint portion). The middle fingerprint portion typically warms up faster than the outer fingerprint portion for a living finger. To the contrary, the outer fingerprint portion of an artificially warmed spoof warms up faster than the middle fingerprint portion. Therefore, the system rejects the applied object as a spoof if the outer fingerprint portion warms up faster than the middle fingerprint portion.

In another embodiment, a predetermined portion of pixels is designated to be the middle fingerprint portion and the surrounding remaining area of pixels is designated as the outer fingerprint portion. For example, a center portion having 150x150 pixels is designated as the middle fingerprint portion and the surrounding remaining area of the 300x300 pixels is designated as the outer fingerprint portion. However, the number of pixels may be modified for different applications.

According to another embodiment, the average intensity is calculated for the middle fingerprint portion and the outer fingerprint portion of each image. The average intensity is calculated in a manner described above with respect to FIG. 1. Specifically, the intensity of the ON-pixels of an image are averaged. The rates of increase, i.e. the average delta average intensity, for the middle fingerprint portion and the outer fingerprint portion, are also calculated for each image. The rates of increase for the middle fingerprint portion and the rate of increase for the outer fingerprint portion are then compared. If the outer fingerprint portion has a rate that is greater than the rate for the middle fingerprint portion, then the system rejects the fingerprint as coming from a spoof. On the other hand, if the middle fingerprint portion has a rate of increase that is greater than the outer fingerprint portion, then the system accepts the fingerprint as coming from a living finger.

In an alternative embodiment, density is calculated for the middle fingerprint portion and the outer fingerprint portion of each image. The density is calculated in a manner described above with respect to FIG. 3. In one embodiment, ON-pixels in a center portion of

BNSDOCID: <WO_ _ 0124700A1_I_>

the image and along the ridges are counted and the density of ON-pixels is then calculated. ON-pixels in an outer portion surrounding the central portion of the image are also counted and the density calculated for each image. The rates of density increase for the middle fingerprint portion and the outer fingerprint portion are also calculated for each image. The rates of increase for the middle fingerprint portion and the rate of increase for the outer fingerprint portion are then compared. If the outer fingerprint portion has a rate that is greater than the rate for the middle fingerprint portion, then the system rejects the fingerprint as coming from a spoof. On the other hand, if the middle fingerprint portion has a rate of increase that is greater than the outer fingerprint portion, then the system accepts the fingerprint as coming from a living finger.

RATE OF WARMING TECHNIQUE

Another way to protect the system from falsely accepting an artificially warmed spoof is to measure the rate of warming due to the applied object and compare it to the rate of warming measured at the time of enrollment or during the subsequent successful verifications for the same finger. The rate of warming, in one embodiment, is calculated using average intensity. For example, average intensity of each captured image is calculated. A successive comparison of the average intensity is done for a currently captured image with the average intensity for a previous captured image. An average delta average intensity representing the rate of warming is then calculated. This rate is then compared with a rate of warming stored in a memory in the system. If the difference between the two rates exceeds a predetermined tolerance, then the system rejects the applied object as a spoof.

In an alternative embodiment, the rate of warming is calculated using density. For example, density of each captured image is calculated. A successive comparison of the density is performed for the density of a currently captured image with the density of a previous captured image. An average delta density representing the rate of warming is then calculated. This rate is then compared with a rate of warming stored in a memory in the system. If the difference between the two exceeds a predetermined tolerance, then the system rejects the applied object as a spoof. Comparing the rate of warming for an applied object and a previously determined rate of warming prevents false acceptance of an artificially warmed spoof because the warming characteristics of a spoof are different than the warming characteristics of a living finger.

BNSDOCID: <WO__0124700A1 I >

RIDGE UNIFORMITY TECHNIQUE

FIG. 4 shows a flowchart for a process where the characteristic associated with perspiration is used to determine whether a fingerprint is from a living finger or a spoof by measuring the changes in intensity along the ridges over a sequence of images. The process starts in step 202. A plurality of images are sequentially captured at a predetermined rate, as is described above (step 204). The intensity along the ridges of each image is measured in step 206. The ridges are again represented by ON-pixels, the ON-pixels being the pixels that have intensities greater than a predetermined threshold.

The intensity along the ridges of each image is compared with intensity along corresponding ridges of a previous captured image successively (step 208). For example, the intensity along ridges of the second image is compared with corresponding intensity along ridges of the first image; the intensity along ridges of the third image is compared with corresponding intensity along ridges of the second image; and so on. If the intensity along the ridges increases in a spatially non-uniform way (step 210), then the system accepts the image as coming from a live person in step 212. This is because a spatially non-uniform increase in intensity along the ridges indicates pores emanating sweat, which is an indicator of a living finger. However, if the intensity along the ridges does not increase in a spatially non-uniform way (step 210), then the image is rejected as coming from a spoof in step 216. The process ends in step 214.

In an alternative embodiment, instead of global measurement of nonuniformly increasing intensity, the nonuniformly increasing intensity is measured along the contours of the ridges to obtain a linear sequence of intensity values. The contours are located by first determining the location of the ridges. The ridges are in turn determined by pixels having intensity values greater than a threshold amount. Pixels having intensities greater than a threshold amount are ON-pixels, as is described above. The image is then binarized, i.e. the ON-pixels are set as black pixels and the rest are set as white pixels. After binarization, the ridge measurement is linear.

A ridge follower (i.e. a computer technique that traces a line through analysis of a string of coterminous pixels) then tracks the ridges on the grayscale image, for example the original image prior to thresholding and binarizing. When the ridge follower is over a pore, the image signal is stronger and the image signal decreases after the ridge follower passed the pore. The signal level tracking a ridge is thus roughly sinusoidal as the signal goes from pore to pore. This nonuniformity in image signals does not exist for a dead or a fake finger

BNSDOCID: <WO__ 0124700A1_I_ >

because they do not have pores. Therefore, the nonuniformity of signals of a ridge indicates vitality. The intensity periodicity and nonuniformity such as frequency may be measured, for example, by Fourier transform.

RIDGE SIGNAL STRENGTH TECHNIQUE

FIG. 5 shows a flowchart for a method of determining whether a fingerprint image is coming from a living finger by determining whether a ridge has maximum signal and the signal does not change. The method starts at box 302 and continues to step 304. In step 304, a sequence of images is captured. The images are compared successively in step 306, using either average intensity or density. If the average intensity or the density of the image does monotonically increase (step 308) and the ridge signals are strong (indicating that the signal is near a maximum value) (step 310), then the system accepts the image as coming from a living finger. In this case, the living finger may be a living finger that is wetted, or a living finger that is saturated due to perspiration caused by heat, exercise, etc. It is noted that a spoof is able to produce a strong signal and may be accepted falsely.

In another embodiment, depending on the security provisions, the system may prompt the user to wipe his finger and try again before accepting the image. In an alternative embodiment, the system may accept the fingerprint without further investigation (e.g. in a lower security application).

If the comparison in step 306 yields a result that the signals between images have changed (step 308), for example the difference is greater than a threshold value, then the system cannot determine whether the image is coming from a living finger (step 316). Similarly, if the signals indicate no change between images and the image does not have a maximum signal value -- i.e., the image strength is as high as the image capture device can measure --, then the system cannot determine whether the image is coming from a living finger (step 316) and the process terminates. The process terminates at box 314.

In one embodiment, instead of ending the process the system continues to look for other characteristics that are indicative of a living finger, such as checking the average intensity as described above in FIG. 1 and/or checking the uniformity of intensity along the ridges over a sequence of images, as described above with reference to FIG. 4.

In sum, the overall objective of the technique is to recognize certain limitations in image capture devices, or image capture means. For instance, due to limitations in the device, there will be circumstances where the initial image has as high a signal strength as the

BNSDOCID: <WO___0124700A1_I_>

device can measure. When this occurs, there is little ability to determine whether the change in image strength over a sequence of images gets stronger, which is a characteristic of a living finger. Accordingly, in one embodiment, gain adjustment techniques, such as those described in U.S. Patent Application Serial No. 09/560,702, filed April 27, 2000, incorporated herein by reference in its entirety above, can be employed when the signal strength is too high -- the gain adjustment technique can lower the image capture device gain and correspondingly lower the strength of the captured images so that a change is detectable. An alternative technique is to measure the signal strength along the middle of the ridges, which is described below in further detail.

WATER DROPLET DIFFERENTIAL TECHNIQUE

FIG. 6 is a flowchart depicting a situation where randomly located water droplets are used to determine whether the fingerprint is coming from a living finger or a spoof. The process starts in box 402 and continues to step 404. In step 404, a sequence of fingerprint images are captured. In step 406, randomly located, i.e. not all located along the ridges, water droplets are identified. Water droplets are indicated by splotches (e.g. globules) -- in this case clusters of pixels in the electrical representation that are representative of a splotch. Because water (at least perspiration) is conductive, water produces a strong signal. The system determines a globule if the ON-pixel area is wider than a ridge (a ridge is usually narrow and long versus a globule that has a larger width). If there is a large number of water droplets, then the applied object is likely either a wetted living finger or a wetted spoof.

The average size of the water droplets of a currently captured image is compared with corresponding water droplets in a previously captured image in step 408. If the water droplet size increases (step 410), then the system accepts the image as coming from a living finger (step 416) and the process ends in step 414. This is because, in general, a perspiring sweat gland creates moisture at a faster rate than the rate at which the skin absorbs the moisture. Hence, for a living finger, the water droplet size increases over time.

If the water droplet size remains static, or decreases over the timed sequence of images (step 410), or is too large, e.g. greater than approximately two or three ridge widths, then two situations may be possible: 1) the applied object is a wetted spoof or 2) the applied object is a living finger with over-accumulation of surface moisture. In either situation, the system does not accept the image as coming from a living finger (step 414), although the system may be falsely rejecting a living finger (as in the second situation).

BNSDOCID: <WO__0124700A1_I_>

In one embodiment, the system notifies the user to remove excessive moisture from the finger, e.g. by wiping the finger, and try again. When the user removes excess moisture from a true finger, the fingerprint will pass under the tests of FIGS. 1, 3, 4 and 5. A spoof, on the other hand, will either continue to fail under the test of FIG. 6 or, if the excessive moisture is removed from the spoof, then the fingerprint will then fail under the tests of FIGS. 1, 3, 4, 7 or 8.

FINGERPRINT VITALITY TECHNIQUE

FIG. 7 shows a flowchart for a method of distinguishing a living finger from a spoof by identifying the vitality of a fingerprint. The vitality is identified by processing a plurality of fingerprints captured over a predetermined period of time.

The process starts at box 502. In step 503 where a first fingerprint image is captured by a fingerprint sensor from an applied object at time zero. A last fingerprint image is captured after a predetermined (and programmable) time in step 504. According to an embodiment, the predetermined time is five seconds. In general, the predetermined time is selected to maximize the differences that can be observed between the captured images over the predetermined time frame. In an embodiment, a sequence of fingerprint images, e.g. nine images, are captured by a fingerprint sensor from the applied object during the predetermined time period. In another embodiment, only the first and the last captured images from the sequence of images are used for classification.

Image differences caused by temporal change in a perspiration pattern are used to determine whether the fingerprint is coming from a living finger or a spoof. More specifically, a living finger perspires, causing the signal pattern to change over time while changes due to perspiration do not occur in a dead or a fake finger. Hence, the finger should not be moisture-saturated when the first image is captured. In one embodiment, if the applied object gives a signal larger than a predetermined level, then the fingerprint verification system prompts the user to wipe his finger to eliminate excess moisture and try again.

Steps 506 through 512 describe a method for obtaining a mask from the last captured image. These steps are exemplary and other techniques can be employed.

The sequence of raw images are then processed through an image processing stage, including noise reduction, image enhancement and contour extraction in step 506, which can include any of the techniques described above, such as that described in U.S. Patent

BNSDOCID: <WO__0124700A1_I_>

Application Serial No. 09/560,702, filed April 27, 2000, entitled "Automatic Gain Amplifier," which is incorporated herein by reference above.

In one embodiment, a blank is captured from the fingerprint sensor, i.e. an image is captured from the fingerprint sensor without a finger placed on the sensor. This blank image represents the static in the background. A fingerprint is then captured from the fingerprint sensor and the blank image subtracted from the captured fingerprint to eliminate the static. In one embodiment, pixels that change within 2% of the blank image are discarded because they are considered to be static noise. In still other embodiments, a median filter can be applied to fill in the white pixels in the middle of the pores and to further smooth the image.

Also in step 506, the last captured image is translated into binary representation. The last captured image is used because a fingerprint from a living finger darkens over time due to increased moisture on the surface of the skin. Therefore, in general, the last captured image has the best contrast, meaning that it has the most defined ridge structure.

In another embodiment, the last captured image is first transformed into grayscale signals, represented by a number of 0 to 255. The last image is then transformed into binary representation by mapping pixels having signals greater than the threshold amount as a black pixel and a pixel having a signal less than a threshold amount as a white pixel.

Binarizing, according to one embodiment, is accomplished with a thresholding circuitry incorporated into the readout circuit of the sensor so that binary outputs are generated from the sense elements. The threshold can be set locally in specific regions of a fingerprint sensor to correct for variations across the sensor. A ridge is identified by the ON-pixels. A valley, on the other hand, is identified by the white pixels.

The binary image is then thinned so that ridges are only one pixel wide (step 508). Thinning reduces the amount of information to be processed to the minimum necessary for the recognition of patterns. In addition, the shape of a thin-line representation of a pattern is more easily analyzed, thus permitting a simpler structural analysis and more intuitive design of recognition algorithms. Preferably, a thinning algorithm compresses data representing the fingerprint, retain significant features of the pattern and eliminate local noise without introducing distortions of its own. Various thinning methods are described by L. Lam et al. in "Thinning Methodologies - A Comprehensive Survey," IEEE Trans. Pattern Analysis and Machine Intelligence, Sept. 1992, pp. 869-885. In general, any suitable method may be used to reduce the number of pixels to a curve of one pixel wide (i.e. a thin line).

3NSDOCID: <WO__ 0124700A1 I >

In one embodiment, a shift is performed after thinning the binary image if the result does not pass through the middle of the original ridges. Shifting is performed because the main part of a ridge is more desirable than the borders of the ridge. The center of the ridges is preferred because the unique features, e.g. pores, of a living finger, reside in the center portion of the ridges rather than the borders of the ridges. Shifting involves moving the thinned line so that it corresponds to the middle of a thicker line from which it came. Preferably, a medial line, that is, one running down the middle of the thicker line, is desired. It is noted that, if thinning is accomplished by medial axis, then no such shifting is needed. The thinned line is moved from its current position so that it intersects midpoints of the thicker line. The midpoints can be determined by creating a line perpendicular to the thick line and identifying a middle point between the intersections of the boundaries of the perpendicular line across the thick line.

The y-connections are removed in step 510 so that the contours only consists of individual curves. A y-connection is where a ridge splits in two (i.e. bifurcates) and has multi-values (each leg of the y is defined by an equation, thus the joint has multiple values). In one embodiment, y-connections are removed by a simple 3x3 non-overlapping neighbor operation.

A 3x3 non-overlapping neighbor operation is useful not only in removing Y-connections, but filtering noise. The 3x3 non-overlapping neighbor operation applies a 3x3 pixel mask (or boundary) centered over a focal pixel (typically an ON-pixel). Thus, there exists a focal pixel and eight neighboring pixels. Next, the system examines each of the neighboring pixels. According to one embodiment, if no neighboring pixel is an ON-pixel, then the focal pixel is assumed to be noise. The process can be repeated for each pixel in the image. Furthermore, focal pixels with only one neighboring pixel that is an ON-pixel can be marked. The marked ON-pixel and focal pixel might, in fact, also be noise. So in a like manner, the marked ON-pixel can be processed as a new focal pixel and, if only one neighboring ON-pixel is found, then the marked ON-pixel and the original focal pixel are probably noise. Likewise, similar coterminous series of ON-pixels, of any desired length, can be eliminated in this manner. Of course, for circumstances greater than two pixel lengths, two neighboring ON-pixels, instead of one, would be the threshold criteria. Pixels assumed to be noise are turned off.

As for circumstances where a y-connection is to be removed, when a focal pixel (an ON-pixel) has two neighbors as ON-pixels, and the neighboring pixels are separated by, for

BNSDOCID: <WO_ 0124700A1_I_>

instance, at least one but not more than two, OFF-pixels, then it is possible that the series of three ON-pixels (the focal pixel and the two neighboring ON-pixels) represents a y-connection. In such a circumstance, the two neighboring ON-pixels are turned off.

After the image is thinned, the resulting contour representing each ridge includes the edge of each ridge (i.e. extremes). Extremes are undesirable because they are not a main part of the ridge but rather on the border of the ridge. As discussed before, the center portion of the ridge contains biological features that are unique to a living finger. Therefore, the end points on a contour (i.e. extremes) are eliminated. The spurs, which are tick marks along ridges (usually a one-bit or a two-bit intrusion), are eliminated as well.

In one embodiment, extremes of the ridges and the spurs are removed using 2-pixel erosion in step 512. A 2-pixel erosion can use the same basic 3x3 non-overlapping neighbor process. Here, a focal pixel has one neighbor. Thus, it is assumed that the focal pixel is an extreme or spur in a ridge. Consequently, the focal pixel is turned off. If extremes or ridges of greater than one pixel are to be removed, then the process can be performed in an iterative manner—once for each additional pixel of the extreme or spur to be removed.

In one embodiment, curves shorter than fifteen pixels are discarded (for instance, using the 3x3 non-overlapping neighbor process described above). Since the nominal pore-to-pore distance is approximately 0.5 mm, spanning approximately ten pixels, a curve shorter than fifteen pixels is too short to capture a pore and their vicinity adequately. At the end of this step, contours roughly follow the center of the ridges of the original captured image and largely contain useful information.

The results from the last captured image are used as a mask in step 514. The mask is placed over the first and the last captured images and the gray scales along the contours (i.e. the mask) of each of the first and last captured images are converted into signals (i.e. strings).

The resulting contours, which traverse through the middle of the ridges, have varying gray levels of the fingerprint image. It is noted that the peaks of the gray levels denote the moist (e.g. pore) locations and the valleys of the gray levels show the dryer regions, usually between each two pores. Typically, there is regularity in the spacing of the pores in a live fingerprint signal. For example, the peak to peak distance in a live fingerprint signal is approximately 10 pixels or 0.5 mm. This is opposed to a fingerprint signal from a dead finger or a plastic finger, which does not have a specific periodicity because a spoof does not have evenly spaced perspiring pores.

BNSDOCID: <WO_ _ 0124700A1_I_>

In step 528, the periodicity of gray levels on each string in the first captured image is measured by a Fourier transform. In one embodiment, the FFT (Fast Fourier Transform) is used because it reveals periodicities (e.g. relative variability) observed across different frequencies of an image. The first captured image is typically "patchy," meaning that when a dry finger is first placed on a fingerprint sensor, gray scale only shows up around the pore areas due to droplets of sweat forming around the pores and the rest of the ridges may not show clearly. Thus, a FFT is done for the first captured image to quantify the variability in gray level along the ridges due to the pores and the presence of perspiration.

A FFT is a known algorithm that is computationally much faster for large numbers of samples in the sequence. Any type of FFT algorithm can be used, for example, mixed radix method, radix 2 method, decimation in time method and the Danlielson-Lanczos Lemma method are all well known and readily available. In another embodiment, a 256-point FFT command is performed. In one embodiment, prior to taking the FFT, the DC signal is removed to eliminate a spike near zero frequency.

The patchiness of a fingerprint changes over time as the ridges become more uniform. This is because sweat emanating from a pore spreads and migrates to dryer parts of the finger. When the last image is taken after a time delay, gray scales typically show up all along the ridges due to moisture spreading towards drier parts of the finger. Thus, there is less variability and a FFT is not performed for the last captured image. Instead, the last captured image is used to extract temporal changes relative to the first capture, which is discussed below.

It is noted that if the finger is already saturated with moisture when the first image is captured, then the first image will not exhibit variability in gray scale. In addition, the last image captured after a time delay will not exhibit sufficient signal change from the first captured image if the finger is initially saturated with moisture. Hence, the finger should not be moisture-saturated when the first image is captured.

For a live fingerprint, the signal representing the first captured image exhibits periodic peaks and valleys having a particular spatial frequency for the peaks. The peaks correspond to pore locations. Also in step 528, the total energy that corresponds to the spatial frequency of the pores is calculated. In general, spatial frequency is defined in cycles/pixel or cycles/mm. The total energy is the approximation of the area under the signal curve that is a result of the FFT. All the numbers in a predetermined window that correspond to spatial distance of approximately 0.4 mm to approximately 1.2 mm are added up, the result of which

BNSDOCID: <WO_ 0124700A1_I_>

is the total energy. Spatial distances of 0.4 mm and 1.2 mm are selected, because as discussed above, the average pore-to-pore distance is approximately 0.5 mm. Assuming a ±0.1 mm variation, for example, the minimum spatial distance is approximately 0.4 mm. A pore may be missing, e.g. a pore that is not sweating. Therefore, the maximum distance between two sweating pores is approximately 1.2 mm.

As discussed before, because a spoof does not have pores, no spatial frequency is available for a spoof. Hence, the total energy for a spoof is of a negligible value, or much less than that of a living finger.

In parallel to step 528 are steps 516 through 526, where temporal changes of a fingerprint are quantified. In step 516, signals representing the contours are connected to form a long signal that represents each of the first captured fingerprint and the last captured fingerprint. The local maximums and local minimums of the first and the last fingerprint signals are detected in step 518. Local maximums are all the different peaks in the long signal and local minimums are all the different valleys in the long signal. Because the long signal exhibits periodic ups and downs, there are multiple peaks and valleys within one signal. This is opposed to a global maximum and a global minimum where only one peak and one valley is selected from the long signal.

The local maximum and the local minimum are used to calculate a series of parameters quantifying the changes caused by the sweating process over time. For live fingerprint signals, the local maximums are typically fairly constant, but the local minimums typically rise over time due to the diffusion of perspiration. In general, the pixels near the pores are relatively saturated while the areas between the pores are relatively dry when the first image is captured, creating fluctuation in the fingerprint signal. However, as time progresses and the sweat diffuses toward dryer regions, the signal becomes more homogeneous (and thus less varying gray level along the ridges). In one embodiment, the series of parameters include total swing ratio (step 520), minimum and maximum growth ratio (step 522), last-first fingerprint signal difference (step 524) and percent change of standard deviation of the first and the last fingerprint signal (step 526). These four parameters are chosen because these four parameters exhibit sufficient differences between a dead and a live fingerprint signal.

In step 520, the total swing ratio of the first fingerprint signal to the last fingerprint signal is calculated. In general, the swing for a live fingerprint is larger than that of a spoof (a fake or dead finger). In addition, the swing is generally smaller for the last captured image

BNSDOCID: <WO 0124700A1_I_>

as compared to the first captured image. As discussed above, moisture begins mainly around the pores creating peaks in the signal. As the time progresses, the moisture gradually spreads along the ridges. Thus, the total swing decreases over time. Because a spoof does not have perspiring pores, this general trend is not present for a spoof fingerprint signal.

Total swing ratio of first captured fingerprint signal to the last captured fingerprint signal is calculated as follows:

$$D.M.1 = \Sigma \left| (C_{1\,i} - C_{1\,i-1}) \right| / \Sigma \left| (C_{2\,i} - C_{2\,i-1}) \right| \quad (1)$$

where C_i is the intensity value of the image at point i along the contour, C_1 denotes the first capture; C_2 denotes the last capture, and the sum is taken for all i=2, 3, ..., C_2 length. It is noted that length C_1 is equal to length C_2 because both the first and the last captured images use the same mask.

In step 522, minimum/maximum growth ratio of first to last fingerprint signal is calculated. As discussed above, for a live fingerprint signal, the height of the local maximums (peaks) increases at a slower rate than the height of the local minimums (valleys). Therefore, the average ratio of the local minimum growth to the local maximum growth is typically larger for a live fingerprint signal as compared to a spoof fingerprint signal. The minimum/maximum growth ratio of first to last fingerprint signal is calculated using the following equation.

$$D.M.2 = \Sigma(C_2{}^{min}{}_j - C_1{}^{min}{}_j) / \Sigma(C_2{}^{max}{}_i - C_1{}^{max}{}_i), \quad (2)$$

where i and j are the maximum/minimum location indexes extracted from the second capture C_2 (the first capture C_1 maximums/minimums are read from the same locations accordingly.)

In step 524, the last-first fingerprint signal difference mean is calculated. Because a nonliving finger does not perspire, the last captured fingerprint signal subtracts the first captured fingerprint signal exhibits a lower degree of change than the signal difference between the first captured fingerprint signal and the last captured fingerprint signal for a living finger. The last-first fingerprint signal difference mean is calculated as follows.

$$D.M.3 = (\Sigma(C_{2\,i} - C_{1\,i})) / n, \; i = 1, 2, ..., n \quad (3)$$

where n = length C_2 = length C_1.

Percentage change of standard deviations of first and last fingerprint signals is calculated in step 526 as follows.

$$D.M.4 = (SD(C_1) - SD(C_2) / SD(C_1)) \quad (4)$$

where SD is Standard Deviation Operator: $SD(X) = (\Sigma(x_i - mean(x))^2 / (n-1))^{1/2}$, n = length X.

BNSDOCID: <WO_ _0124700A1 I >

If the signal fluctuation decreases around the means, which is typical for a live fingerprint signal, then the percentage change of standard deviation would rise. Hence, a higher value of percentage change of standard deviations of the first and the last fingerprint signals indicates a living finger.

The results from steps 520 through 528 are then fed into a back-propagation neural network classifier. In step 530, a decision on vitality is made in accordance to the results from the back-propagation neural network classifier. It is noted that the back-propagation neural network classifier can classify a fingerprint signal based on any one of these five measurements. However, a combination with one or more other measurements can produce better classification precision and thus a more robust system than using one measurement alone.

A neural network is a software (or hardware) simulation of a biological brain. One advantage a neural network has over digital computers is the ease of taking into account high-order statistical relationships of stochastic data. More specifically, a neural network learns to recognize patterns in an input data by utilizing the principle of reward and punishment, by back-propagating the needed information for altering structures of interconnections and strength or weights of these interconnections dynamically. Once the neural network has been trained on samples of input data, it can make predictions by detecting similar patterns in future data.

The architecture of a back-propagation neural network consists of two major components: nodes and the connections between the nodes. The back-propagation neural network is a multi-layered network, with the output from one layer serving as input to the next. The layers with no external output connections are referred to as hidden layers. A back-propagation network with a single hidden layer consists of three layers of nodes (input, hidden, and output) and full interconnection between input and hidden layers and the hidden and output layers. Residing on these connections are weights that multiply signals passing over the connection. The product of the signal magnitude and weight is summed over all connections leading to a particular node to give the initial output for that neuron (the actual result is dictated by the activation function chosen for the node). In general, the number of hidden layer neurons should be approximately one-half of the input layer nodes.

Training begins with all weights set to random numbers. For each data record, the predicted value is compared to the desired (actual) value and the weights are adjusted to move the prediction closer to the desired value. Many cycles are made through the entire set

BNSDOCID: <WO___0124700A1_I_>

of training data with the weights being continually adjusted to produce more accurate predictions. In one embodiment, a back-propagation neural net (three layer perceptron), with sigmoid non-linearity, is used.

Training a neural network requires the use of the same parameters that will be used to make the classification. Training involves, for example, different data sets of the five parameters from subjects in each classification. For instance, one classification may be a living finger, one classification may be a dead finger, and one classification may be a plastic finger. In another instance, twelve data sets are collected from each class. According to one embodiment, the training algorithm uses gradient descent in conjunction to batch input-output training vectors to classify the input cases as live or spoof. In another embodiment, bipolar targets (+1, -1) are chosen to denote live and spoof, respectively.

If the output of the back-propagation neural network indicates that the fingerprint is from a living finger (step 532), then the system passes the fingerprint as coming from a living finger (step 540) and the process ends in step 544. However, if the output of the back-propagation neural network indicates that the fingerprint is from a spoof (step 532), then it is determined whether the number of trials is equal to a predetermined number, e.g. 3 (step 534).

If the number of trials has reached the predetermined number, then the system indicates that the fingerprint failed and cannot be accepted as coming from a live person (step 542). The process ends in step 544. It is noted that each time input data travels through the back-propagation neural network, a counter recording the number of trials is incremented by one. The counter is reset at the end step 544.

If the number of trials has not reached the predetermined number, then the system prompts the user to wipe his finger and try again in step 536. The process repeats by returning to the start step (step 538).

INVERTED SPOOF DETECTION TECHNIQUES

Turning to FIG. 8, it depicts a method for distinguishing between a real fingerprint and an inverted spoof of the fingerprint. An inverted spoof is created when the ridge and valleys of an enrolled fingerprint are essentially turned inside-out. The inverted spoof is a fairly simple technique for fooling a fingerprint capture system. Indeed, it can be particularly powerful: turning contour of the finger inside-out maintains the ridges and valleys -- or at

BNSDOCID: <WO__0124700A1 I >

least their transition points (endpoints and bifurcations), which is what is compared according to an embodiment of the system.

In order to detect an inverted fingerprint, characteristics of the transition points are analyzed and compared between the enrolled fingerprint data and the captured fingerprint data. More particularly, and in the embodiment described below, when a fingerprint contour is inverted, the bifurcations become endpoints and vise-versa; the system, accordingly, performs a statistical analysis on the ratio of bifurcations to endpoints, with respect to matching minutiae, to detect the inversion.

In step 804, the fingerprint sensor captures an image of the applied object (the finger). In step 808, minutiae are compared between the captured image and an enrolled image. A test is performed in step 812 to determine whether a match was found in step 808. If a match was found then, in step 816, a match counter is incremented (once for each match if multiple minutia are compared in step 808).

In step 820, the matching minutiae are classified by type by extracting information from the image. By classifying each minutia by type it is meant is endpoints and bifurcations are so marked. If the matching minutiae of the enrolled image have not already been classified, then they are classified too. According to one embodiment, to classify the minutiae by type, the 3x3 non-overlapping neighbor technique, described above, can be employed. Y-connections (bifurcations) can be extracted by examining at least three ON-pixels in the proximity of the minutia, while endpoints can be extracted by examining at least two ON-pixels in the proximity of the minutia. If the image has been filtered, in accordance with the process described above with reference to FIG. 7, then such information can be extracted then, rather than in a separate step as is depicted in FIG. 7.

In step 824, a test is performed to determine whether the captured and enrolled minutiae are of the same type. If they are not, then a type mismatch counter is incremented in step 828. If they are, or after step 828, then a next test (step 832) determines whether there are more minutia that need to be compared. If there are more minutiae to be compared, then a next minutiae is retried in step 836 and processing continues to step 808. If there are no more minutiae to be compared, then in step 840 the ratio of the type mismatch counter value to the match counter value is calculated.

A test is performed in step 844 to determine whether the calculated ratio exceeds a threshold value. According to one embodiment, the threshold value is 50%. This is because the inventors have found that due to potential non-uniformities in, for instance, a capacitive

BNSDOCID: <WO___0124700A1_I_>

fingerprint sensor, and/or environmental conditions, a number minutiae will be misclassified -- in particular where pixel intensity at or near an endpoint or bifurcation is just below the ON-pixel threshold value. The threshold value, can however, be reduced to a much lower tolerance if proper filtering or more ideal environmental conditions are present.

If the ratio exceeds the threshold, then in step 848 the captured image is rejected as an inverted spoof. Otherwise, in step 852, the captured image is identified as not being an inverted spoof and the captured image is either accepted, or other security constrains enforced.

ADDITIONAL TECHNIQUES

Additional tests may be executed to deal with varying environmental conditions. In one embodiment, the rate of effects under different environmental conditions is compared with the rate of effects under ambient conditions, such as temperature and humidity, for adjustment of certain predetermined parameters. For example, the rate of heating in freezing temperature and the rate of heating in extreme heat differ from the rate of heating under ambient temperature. Another example is that the rate of heating in dry weather and the rate of heating in humid weather differ from the rate of heating under ambient condition. Because the rate of heating varies under different environmental conditions, the minimum time and the maximum time for determining whether a fingerprint is coming from a living finger, for example, are modified according to the ambient conditions. For example, in cold weather, instead of a minimum time of 1.2 seconds, the system waits for 3 seconds and instead of a maximum time of 3 seconds, the system allows for 5 seconds to determine whether the finger is alive.

In one embodiment, pore placement is measured along the ridges to detect whether the pore pattern matches that of the true enrolled finger or a previously successfully verified finger. Pore placement can be measured directly or by locations of the sweat droplets as described above. More specifically, in one embodiment, pores are detected by detecting the peaks of a sinusoidal curve. Since the pores are very shallow and small, their fine features are not easily replicated by a spoof. Hence, pore placement may be a test for a true, versus a fake, finger.

In another embodiment, a global measurement of the texture of a finger is performed and the result compared with the texture of a finger measured during enrollment or measured during a previous successful verification. The skin of a living finger has very fine features

BNSDOCID: <WO__0124700A1 I_>

that cannot be easily reconstituted in a rendition of that finger. These fine features may be, for instance, measured and quantified by using Fourier transform and looking at the high frequency details. A living finger, in general, has higher frequency details then a plastic finger. The texture measured may be, but not limited to, pores and other small texture that cannot be readily and reliably reproduced. In one embodiment, the textures may be measured using a device that measures very fine features.

According to another embodiment, a biomedical measurement device is used to measure certain characteristics of a living finger, such as, but not limited to, skin resistance, temperature, pulse-oximetry (blood oxygen measured by absorption of near infrared light and red light), electrocardiogram (electrical potential changes of cardiac activity versus time), laser Doppler measurement of blood flow, x-ray, pressure and other physiological vitality indicators. These measurements are compared with corresponding measurements taken during enrollment or during a previous successful verification.

In still another embodiment, the system is a multi-modal system which requires more than one biometric measurements such as, but are not limited to, fingerprint, voice, hand-writing, retina, etc. By using a multi-modal system, an attacker must obtain multiple tools to manufacture different modes of spoof, thus making a spoof attack more difficult.

According to another embodiment, the system requests a user to put the same finger down on the capture device twice. A sequence of images is captured for each application. The first and the second sequence of images are then compared. It is noted that the fingerprint images from a living finger exhibit some hysteresis as the characteristics change. In particular, the first of the second sequence of images exhibits characteristics closer to the last image of the first sequence of images. The first image of the second sequence of images from a spoof, on the other hand, displays characteristics that are closer to the first image of the first sequence of images captured from the initial application. This difference is due to the fact that a finger has an elastic surface, thus the surface of the finger stretches and varies under different conditions. Hence, the closer in time the fingerprints are taken, the closer the images. In contrast, a molded finger typically produces identical fingerprints during initial application. Therefore, by comparing the images from two different applications, the system is able to determine whether the applied object is a living finger.

Although the invention has been described with reference to particular embodiments, the description is only an example of the invention's application and should not be taken as a

BNSDOCID: <WO__0124700A1_I_>

limitation. For example, other types of classifier may be used to classify the fingerprint signals. For instance, a classifier may be devised using the median values derived from a training set to determine a threshold. The classifier may than accept or reject a fingerprint signal based on the threshold value. Various other adaptations and combinations of features of the embodiments disclosed are within the scope of the invention as defined by the following claims.

In one embodiment, the system can include an algorithm that randomly selects and requests one or more fingers for measurements, the maximum allowable number of fingers requested being ten. Randomly requesting different and varying number of fingers makes the attack more difficult because it is more difficult for an attacker to manufacture multiple spoofs. Furthermore, any of the particular spoof detection techniques described above can also employed, on a case-by-case basis, to detect a spoof. Since the selection of the finger and/or algorithm is random, it adds unpredictability (with respect to potential spoofers), thus making the system more resistant to attacks.

BNSDOCID: <WO__0124700A1 I >

CLAIMS

What is claimed is:

1. A biometric sensing system comprising:

an image capture device configured to sample an applied object and create an electrical representation of the applied object; and

a spoof detection module configured to analyze the electrical representation of the applied object for relative intensity, density, geometric, or temporal anomalies indicative of a non-living applied object.

2. The biometric sensing system of claim 1, wherein the spoof detection module employs an average intensity technique to detect and classify the anomalies, the average intensity technique configured to cause the system to capture a plurality of images of the applied object, and calculate an average intensity for each of the plurality of captured images.

3. The biometric sensing system of claim 2, wherein the average intensity technique is further configured to cause the system to reject the applied object as a spoof when the average intensity does not increase monotonically over the plurality of images.

4. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a pixel density technique to detect and classify the anomalies, the pixel density technique configured to cause the system to capture a plurality of images of the applied object, determine an ON-pixel value based upon a first captured image, determine a pixel count for each image in the plurality of captured images, wherein the counted pixels exceed the ON-pixel value, and calculate a delta pixel count value over the plurality of images.

5. The biometric sensing system of claim 4, wherein the pixel density technique is further configured to cause the system to reject the applied object as a spoof when the delta pixel count does not increase monotonically over the plurality of images.

6. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture a plurality of images of the

BNSDOCID: <WO___0124700A1_I_>

applied object, measure pixel intensity along ridges in each of the plurality of captured images, determine whether the pixel intensity increases in a spatially non-uniform manner, and reject the applied object as a spoof when the pixel intensity does not increase in the spatially non-uniform manner.

7. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture a plurality of images of the applied object, measure pixel intensity along ridges in each of the plurality of captured images, determine whether the pixel intensity increases in a spatially non-uniform manner, and reject the applied object as a spoof when the pixel intensity does not increase in the spatially non-uniform manner.

8. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a ridge uniformity technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture a plurality of images of the applied object, measure pixel intensity values along contours of ridges in each of the plurality of captured images, binarize the pixel intensity values, measure pixel intensity variations along the ridges, and reject the applied object as a spoof when the measured pixel intensity variations are not roughly sinusoidal.

9. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a water droplet differential technique to detect and classify the anomalies, the ridge uniformity technique configured to cause the system to capture an image of an applied object, locate a first water droplet positioned within the image, capture a subsequent image of the applied object, locate a like-positioned water droplet within the subsequently captured image, compare a size of the first water droplet with a size of the like-positioned water droplet, and reject the applied object as a spoof when the size of the like-positioned water droplet is smaller than the size of the first water droplet.

10. The biometric sensing system of any of the above claims, wherein the spoof detection module employs a fingerprint vitality technique to detect and classify the anomalies, the fingerprint vitality technique configured to cause the system to capture a plurality of images

BNSDOCID: <WO_ 0124700A1 I >

of an applied object, digitally process the plurality of captured images, form a fingerprint signal representative of fingerprint strings from each of the plurality of images, compare changes between the fingerprint signal corresponding to an initial image in the plurality of images and a fingerprint signal from a subsequently captured image in the plurality of images, and reject the applied object as a spoof when the changes exceed a threshold amount.

11. The biometric sensing system of claim 10, wherein the fingerprint vitality technique is further configured to cause the system to compare a total swing ratio of the fingerprint signal of the initial image and the fingerprint signal of the subsequently captured image.

12. The biometric sensing system of claim 10 or 11, wherein the fingerprint vitality technique is further configured to cause the system to compare a minimum or a maximum growth ratio as between the fingerprint signal of the initial image and the fingerprint signal of the subsequently captured image.

13. The biometric sensing system of claim 10, 11 or 12, wherein the fingerprint vitality technique is further configured to cause the system to compare last to first fingerprint signal difference mean between the plurality of images.

14. The biometric sensing system of claim 10, 11, 12 or 13, wherein the fingerprint vitality technique is further configured to cause the system to compare a percentage change of standard deviations between the fingerprint signal of the initial image and the fingerprint signal of the subsequently captured image.

15. The biometric sensing system of claim 10-14 or 15, further comprising a neural network, wherein the neural network configured to perform the steps of comparing.

16. The biometric sensing system of any of the above claims, wherein the spoof detection module is configured to extract minutia type information from the electrical representation, compare minutia type information with information corresponding to an enrolled object, calculate a ratio of mismatched minutia type information to matching minutia information, and reject the applied object as an inverted spoof when the ratio exceeds a threshold type mismatch ratio.

BNSDOCID: <WO_ 0124700A1_I_>

17. The biometric sensing system of any of the above claims, further comprising a minutia matching module configured to compare minutiae extracted from the electrical representation of the applied object with minutiae of an enrolled object.

18. The biometric sensing system of any of the above claims, wherein the image capture device is a capacitive fingerprint sensor.

19. A computer implemented method for detecting a spoof of a living finger, comprising:

receiving one or more electrical representations representative of a plurality of images of an applied object; and

analyzing the one or more electrical representations for relative intensity, density, or geometric anomalies indicative of a non-living applied object.

20. The method of claim 19, wherein the step of analyzing comprises:

calculating an average intensity for each of the plurality of images; and

rejecting the applied object as a spoof when the average intensity, as sequentially measured over the plurality of images, does not increase monotonically.

21. The method of claim 20, further comprising:

calculating an average change in the average intensity of the plurality of images; and

rejecting the applied object as a spoof when the average change in the average intensity is below a threshold average change in the average intensity value.

22. The method of claim 19, 20 or 21, wherein the step of analyzing comprises:

selecting a portion of a first image in the plurality of images;

determining an ON-pixel value based upon intensity values in the portion of the first image;

counting a number of pixels exceeding the ON-pixel value in the portion of the first image;

repeating the above steps of selecting, determining, and counting for a next image in the plurality of images;

calculating an average density value between the first image and the next image; and

BNSDOCID: <WO__0124700A1 I >

rejecting the applied object as a spoof when the average density value is not increasing monotonically.

23. The method of claim 22, further comprising:

calculating an average change in average density between the plurality of images; and

rejecting the applied object as a spoof when the average change in average density is less than a threshold average change in average density value.

24. The method of claim 19, 20, 21, 22 or 23, wherein the step of analyzing comprises:

measuring intensity along ridges in each of the plurality of images;

comparing the intensity along the ridges from each captured image with the intensity along the ridges from a coterminously captured image;

determining whether the intensity along the ridges increases in a spatially non-uniform manner; and

rejecting the applied object as a spoof when the intensity along the ridges does not increase in a spatially non-uniform manner.

25. The method of claim 19, 20, 21, 22, 23 or 24, wherein the step of analyzing comprises:

comparing the electrical representations of each of the plurality of images for changes;

comparing maximum signal values in the electrical representations when there are insignificant changes between the electrical representations;

rejecting the applied object as a spoof when the electrical representation holds signal values indicative of insignificant changes between successive images.

26. The method of claim 19, 20, 21, 22, 23, 24 or 25, wherein the step of analyzing comprises:

locating water droplets in each of the plurality of images;

comparing a size of the water droplet in each of the plurality of images with a size of the water droplet in a subsequently captured image in the plurality of images;

rejecting the applied object as a spoof when the water droplet size is static or decreases, over time, as represented in the plurality of images.

BNSDOCID: <WO___0124700A1_I >

27. The method of claim 19, 20, 21, 22, 23, 24, 25 or 26, wherein the step of analyzing comprises:

digitally processing a first electrical representation;

saving the digitally processed electrical representation as a mask;

applying the mask over subsequent electrical representations;

converting the result of the mask of the subsequent electrical representations into fingerprint strings;

connecting the fingerprint strings into a fingerprint signal for each image;

analyzing the fingerprint signal for anomalies; and

rejecting the fingerprint signal when the anomalies are not indicative of a living finger.

28. The method of claim 27,

wherein analyzing the fingerprint signal for anomalies comprises calculating a total swing ratio of a first fingerprint signal to a last fingerprint signal; and

rejecting the fingerprint signal when the total swing ratio is not indicative of a living finger.

29. The method of claim 27 or 28,

wherein analyzing the fingerprint signal for anomalies comprises: calculating a minimum or maximum growth ratio as measured between a first fingerprint signal and a last fingerprint signal; and

rejecting the fingerprint signal when the growth ratio is not indicative of a living finger.

30. The method of claim 27, 28 or 29,

wherein analyzing the fingerprint signal for anomalies comprises calculating a first fingerprint signal to a last fingerprint signal difference mean; and

rejecting the fingerprint signal when the signal difference mean is not indicative of a living finger.

31. The method of claim 27, 28, 29 or 30,

BNSDOCID: <WO 0124700A1_I_>

wherein analyzing the fingerprint signal for anomalies comprises calculating a percentage change of standard deviation between a first fingerprint signal and a last fingerprint signal; and

rejecting the fingerprint signal when the signal difference mean is not indicative of a living finger.

32. The method of claim 27, 28, 29, 30 or 31, further comprising:

calculating a spatial frequency of peaks in the fingerprint strings;

calculating a total energy for the fingerprint strings, based on the spatial frequency; and

rejecting the fingerprint signal as a spoof when the average energy is below a threshold total energy.

33. The method of claim 27, 28, 29, 30, 31 or 32, further comprising, prior to rejecting the fingerprint signal as a spoof, sending the anomalies to a neural network for classification.

34. The method of claim 19-32 or 33, wherein the step of analyzing the one or more electrical representations comprises:

extracting minutia type information from the electrical representation;

determining whether the minutia type information matches a minutia type of a matching minutia from an enrolled finger;

calculating a ratio of mismatched minutia types to matching minutia; and

rejecting the fingerprint signal as a spoof when the ratio of mismatched minutia types to matching minutia exceeds a threshold mismatch value.

35. The method of claim 19-33, or 34, further comprising:

capturing the plurality of images of the applied object with a fingerprint sensor; and

converting the plurality of images into the one or more electrical representations of the applied object.

36. The method of claim 35, wherein the fingerprint sensor captured the plurality of images with a capacitive fingerprint sensor.

BNSDOCID: <WO___0124700A1_I_>

37. The method of claim 19-35, or 36, further comprising matching minutiae extracted from at the one or more electrical representations with minutiae from an enrolled finger.

38. A computer software product having stored therein one or more sequences of instructions for causing one or more processors to perform any of steps as recited in any of above claims 19 through 37.

SNSDOCID: <WO__ 0124700A1 I >

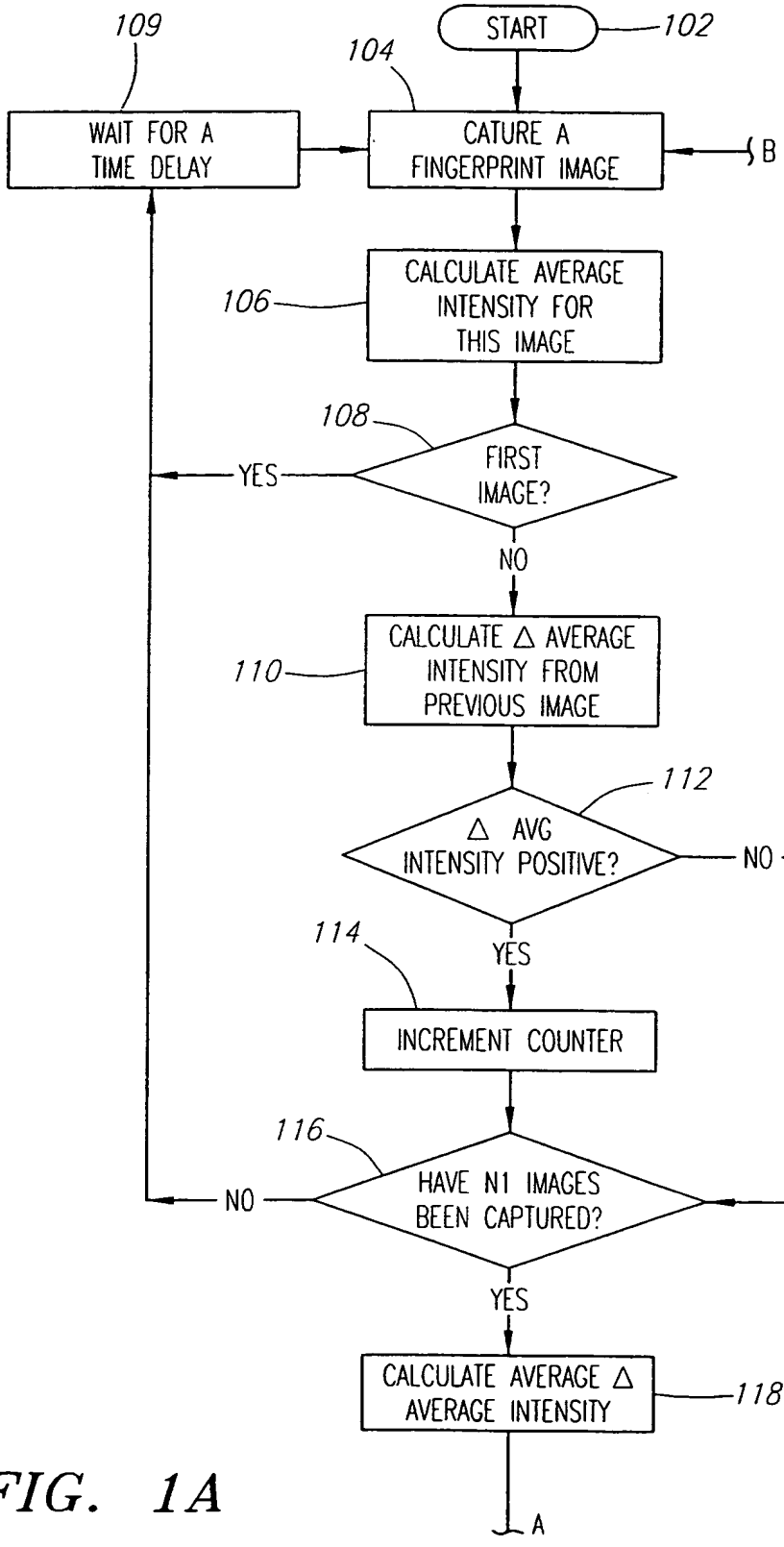


FIG. 1A

FIG. 1B

FIG. 1

BNSDOCID: <WO___0124700A1_I_>

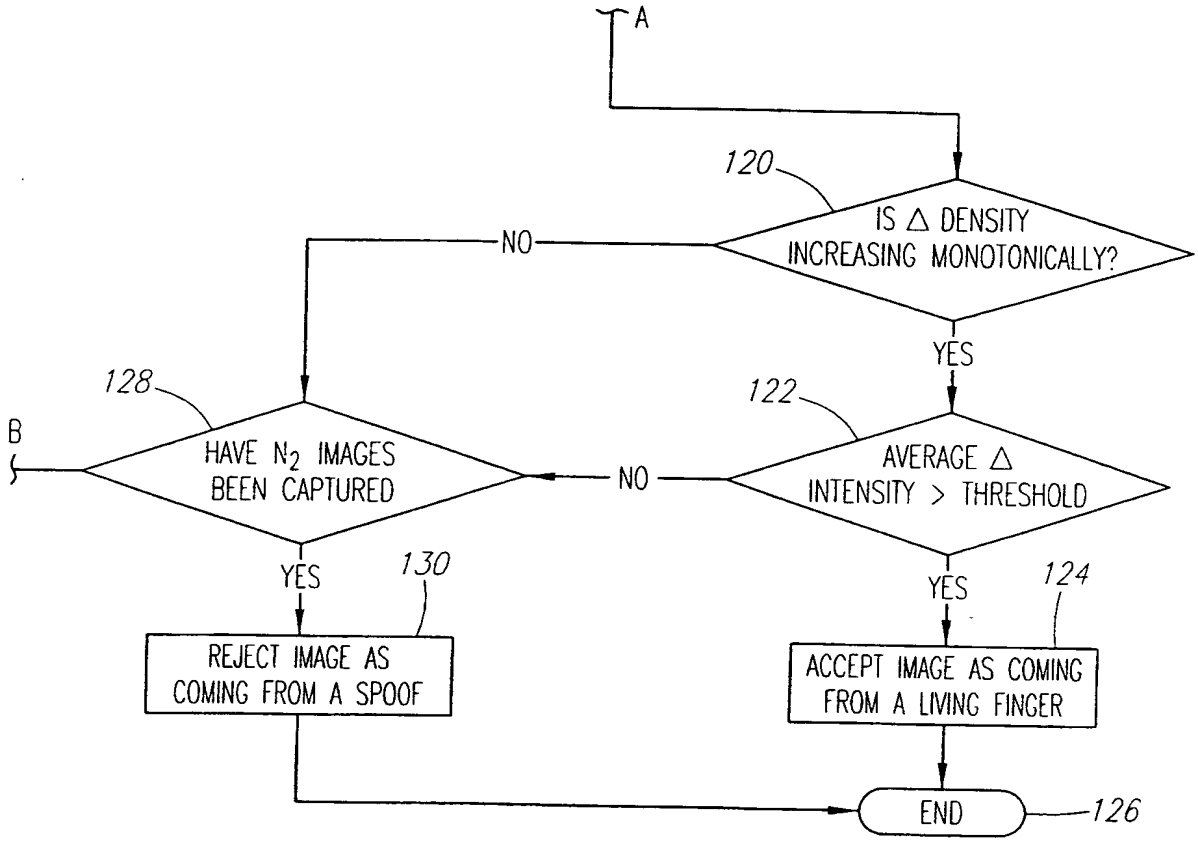


FIG. 1B

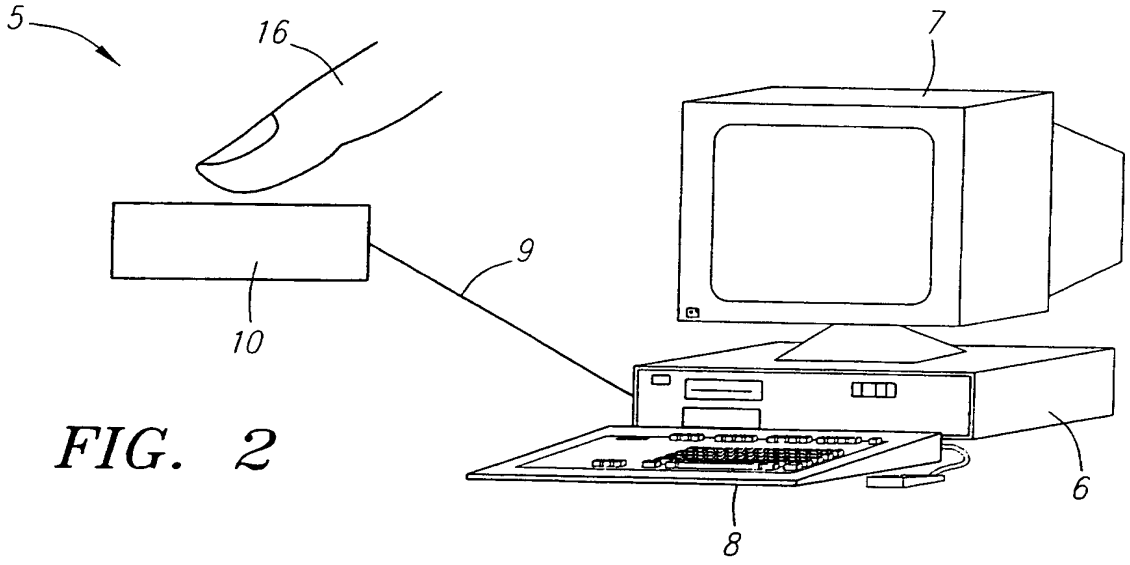


FIG. 2

NSDOCID: <WO___0124700A1_I_>

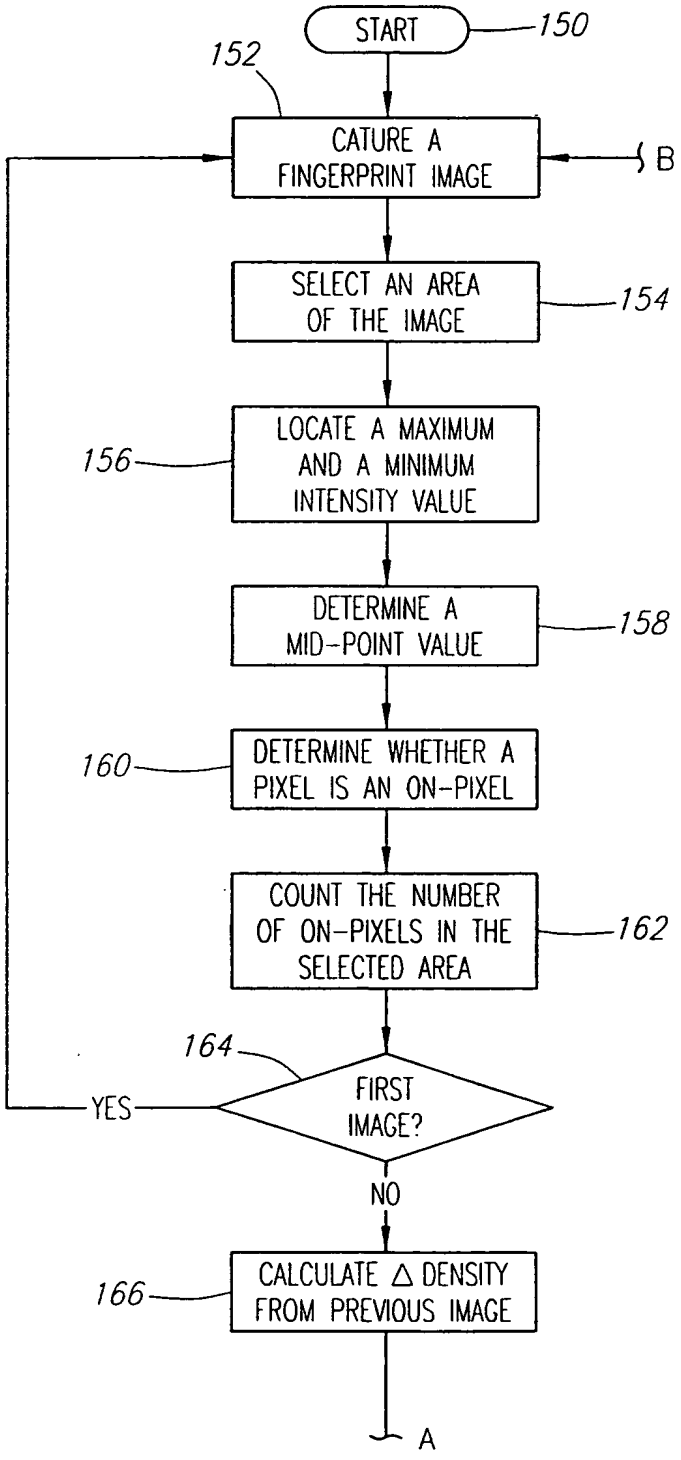


FIG. 3A

FIG. 3A

FIG. 3B

FIG. 3

BNSDOCID: <WO___0124700A1_I_>

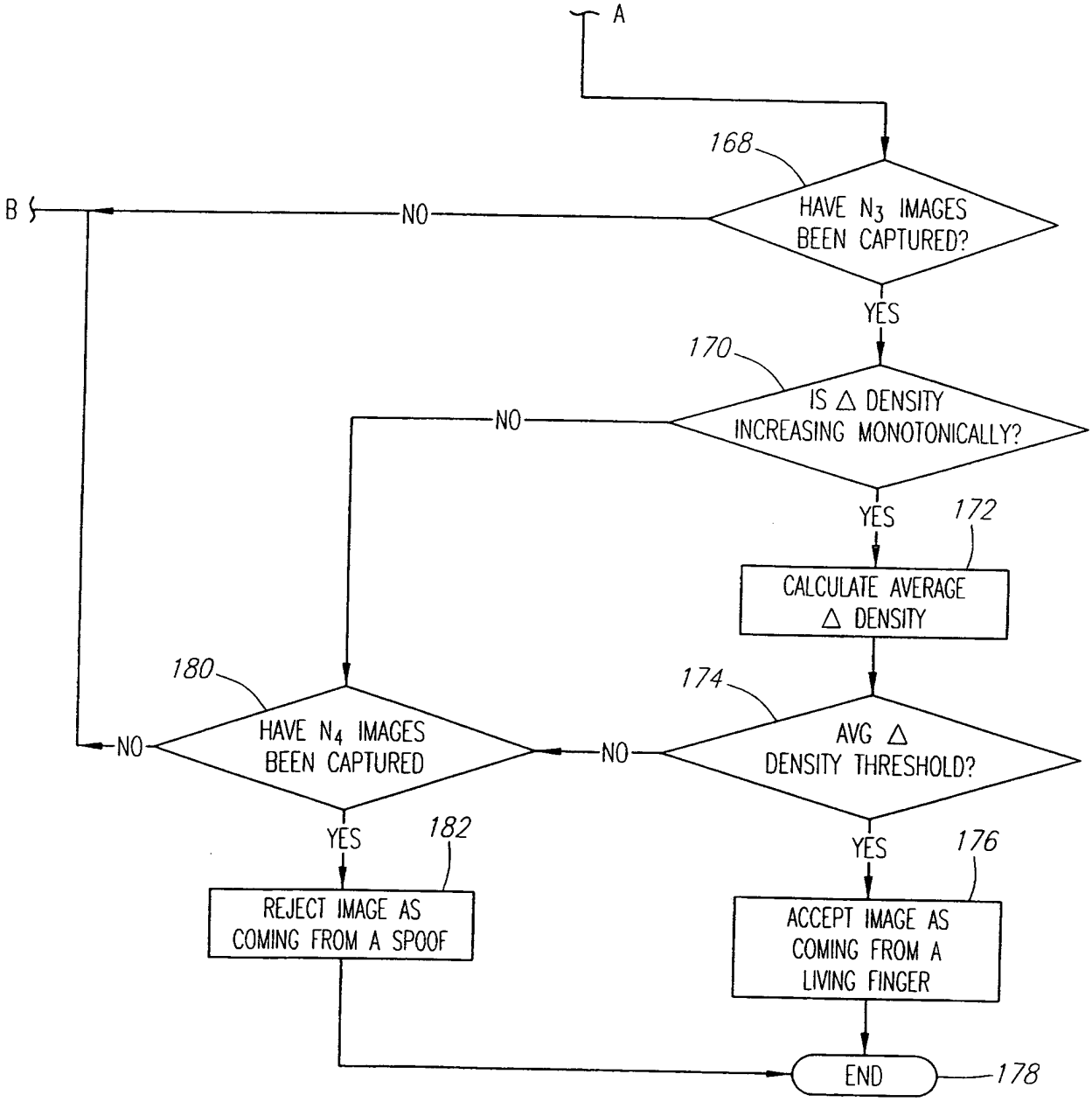


FIG. 3B

SDOCID: <WO___0124700A1_I_>

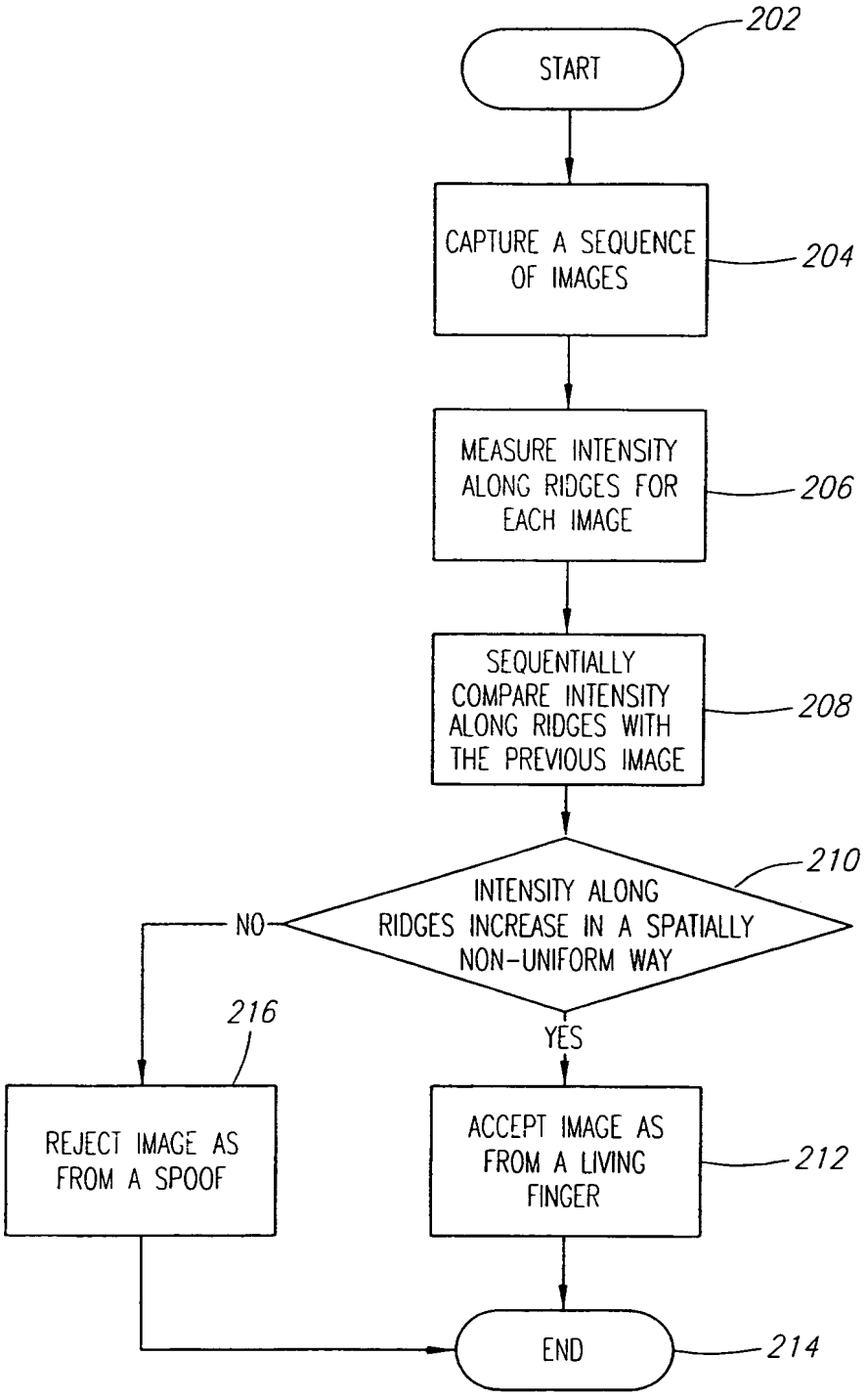


FIG. 4

BNSDOCID: <WO___0124700A1_I_>

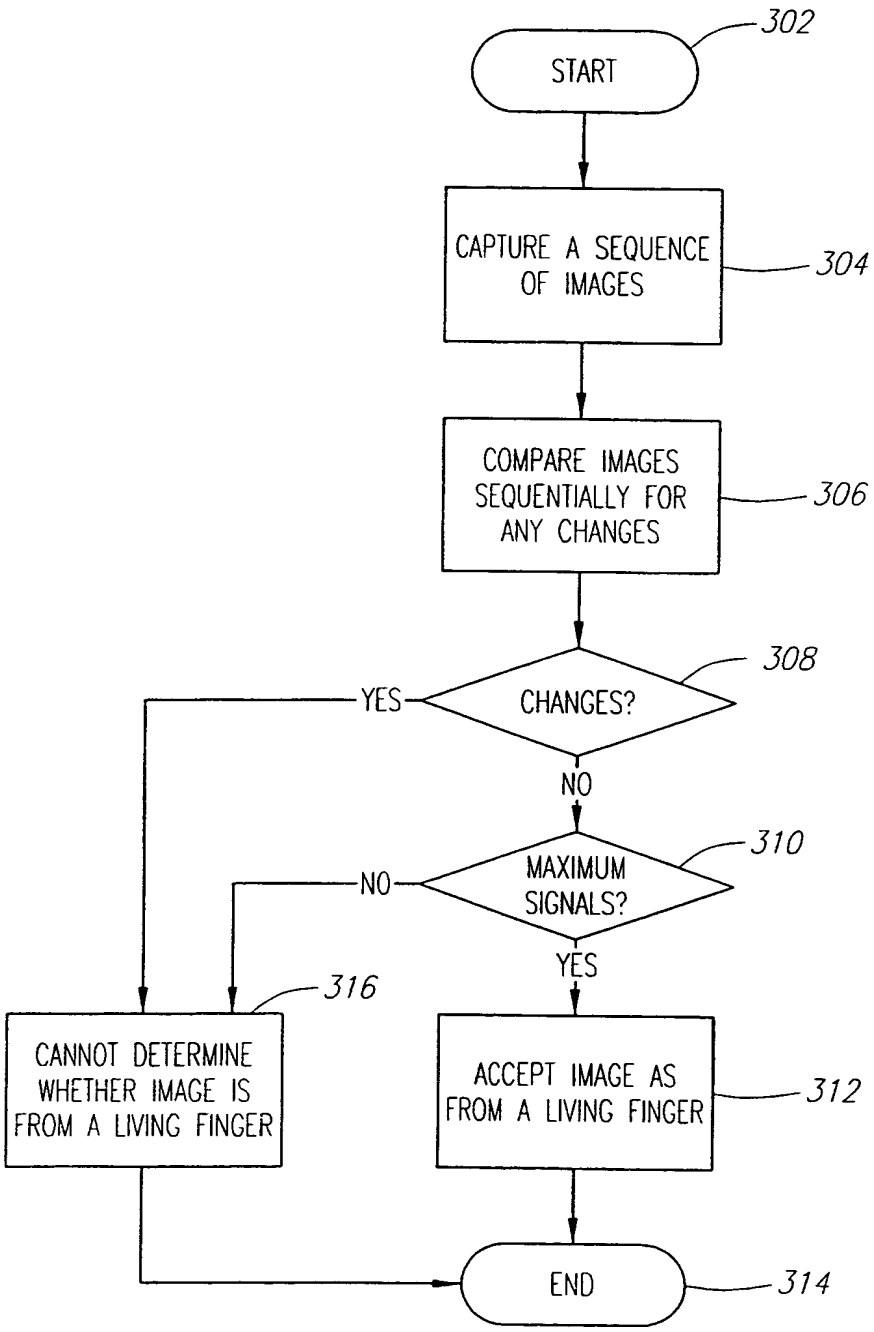


FIG. 5

BNSDOCID: <WO___0124700A1_I_>

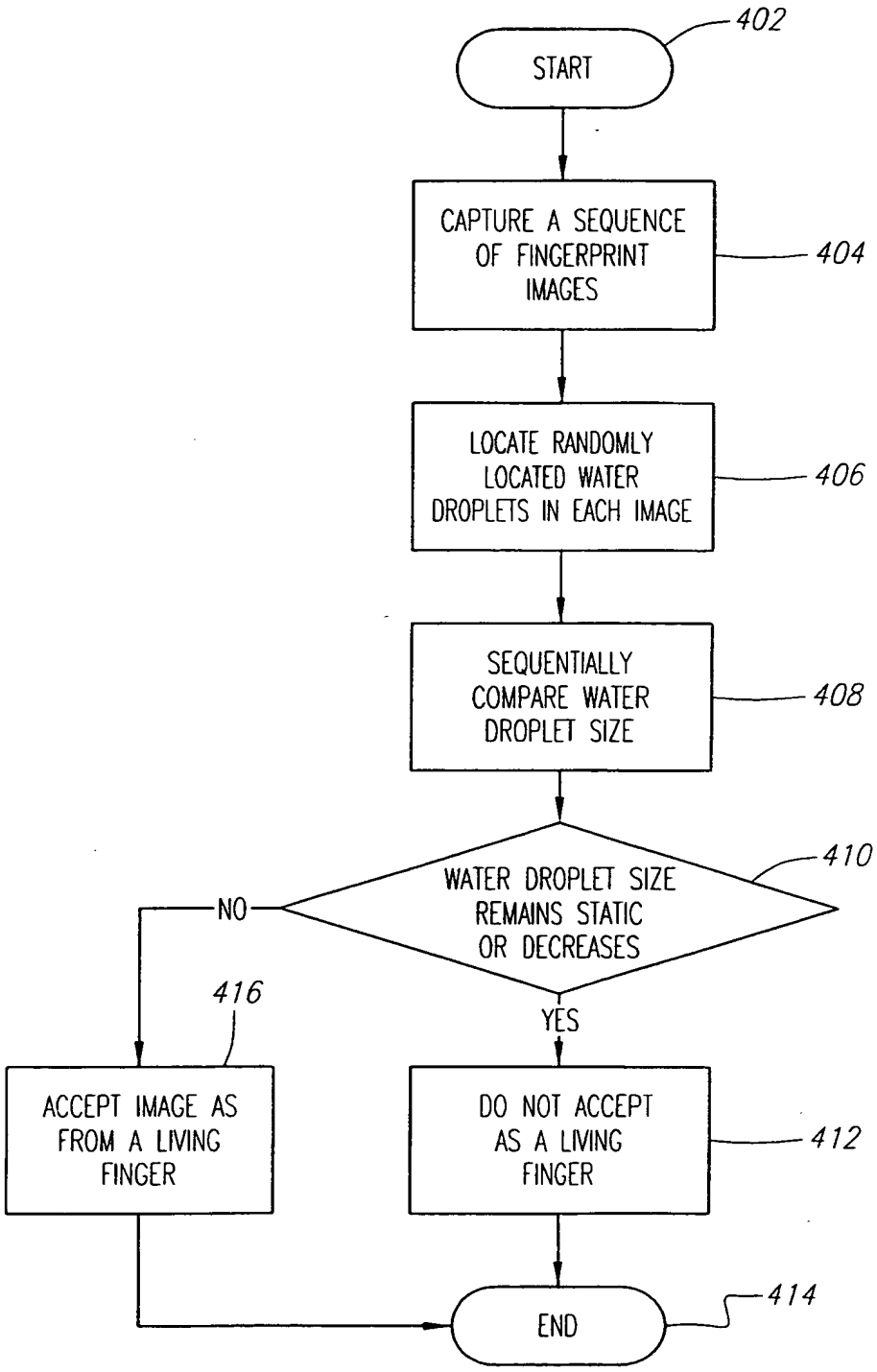


FIG. 6

BNSDOCID: <WO___0124700A1_I_>

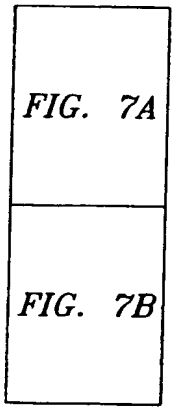


FIG. 7

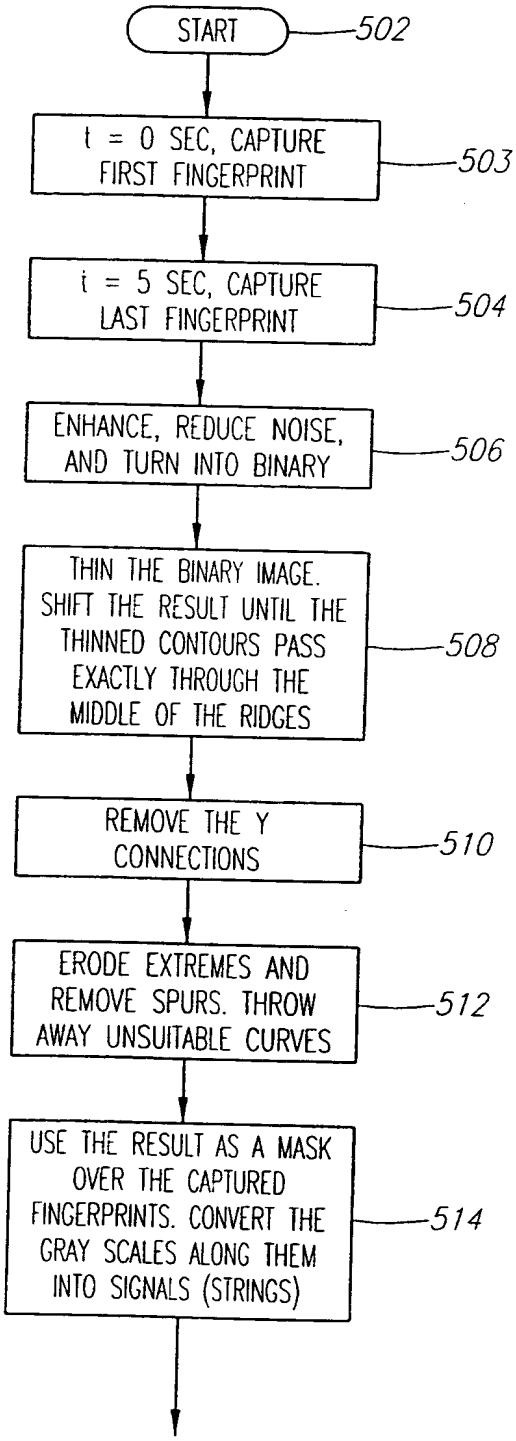


FIG. 7A

BNSDOCID: <WO___ 0124700A1_I_>

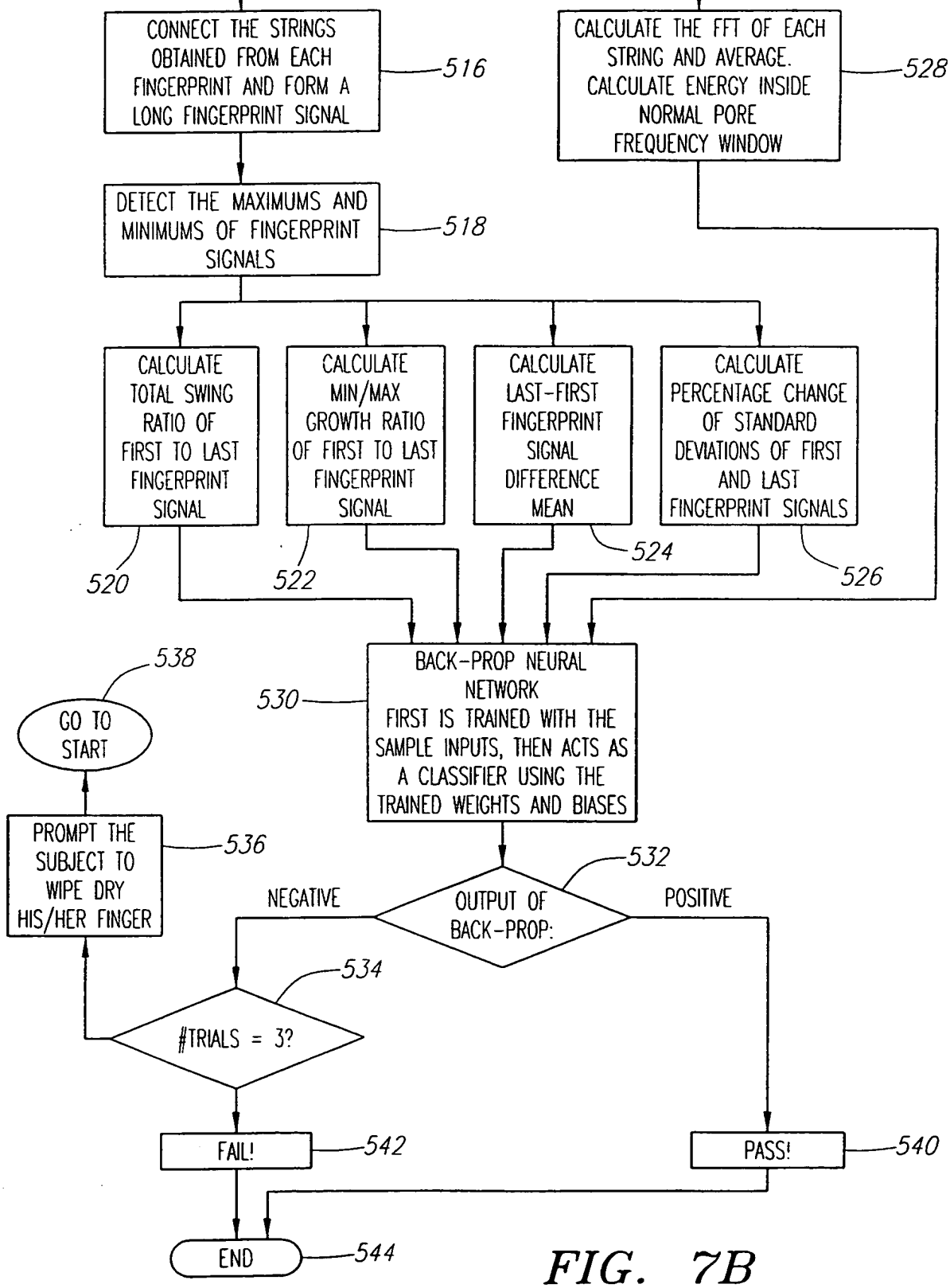


FIG. 7B

BNSDOCID: <WO___0124700A1_I >

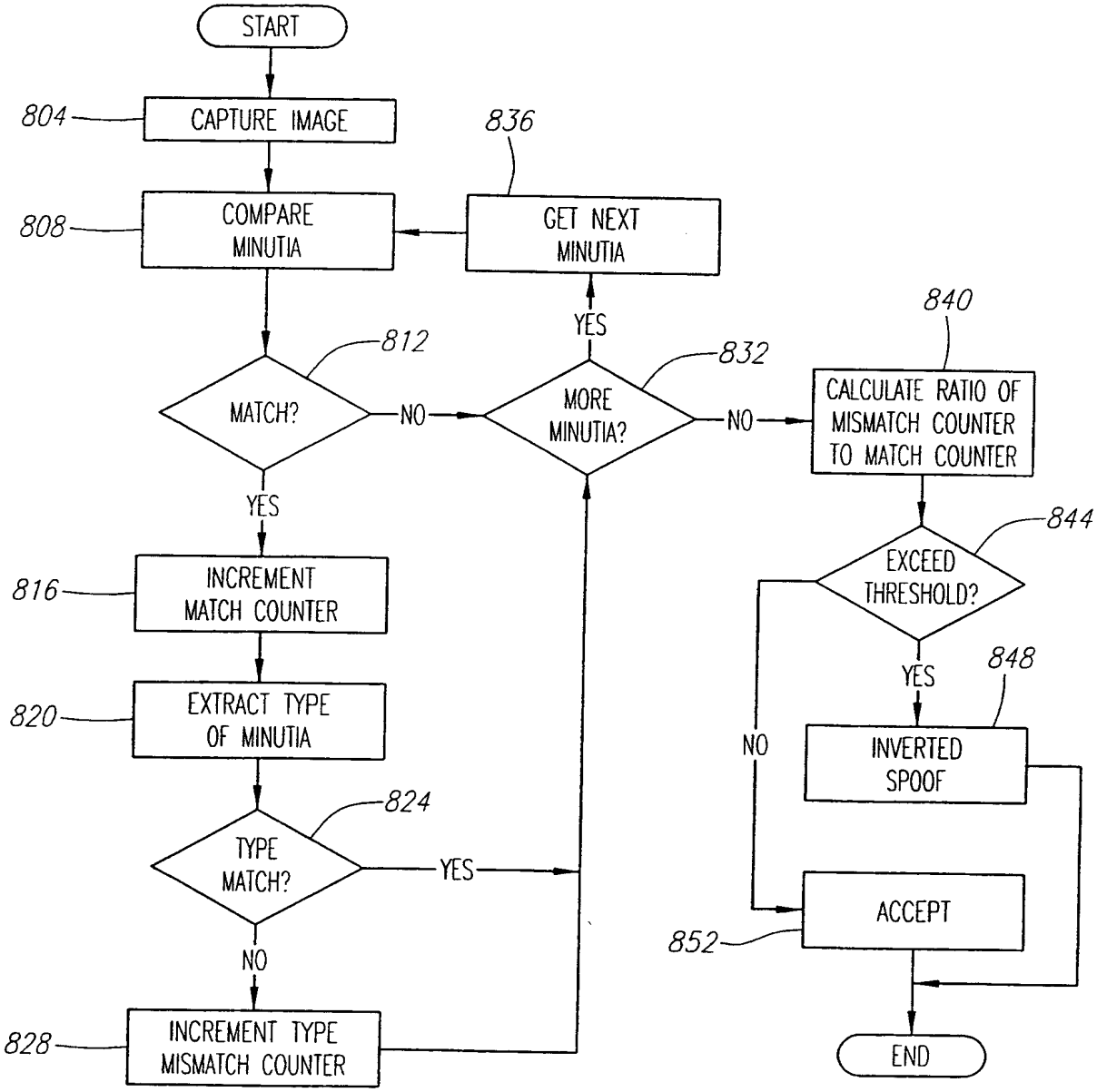


FIG. 8

BNSDOCID: <WO__ 0124700A1_I_>

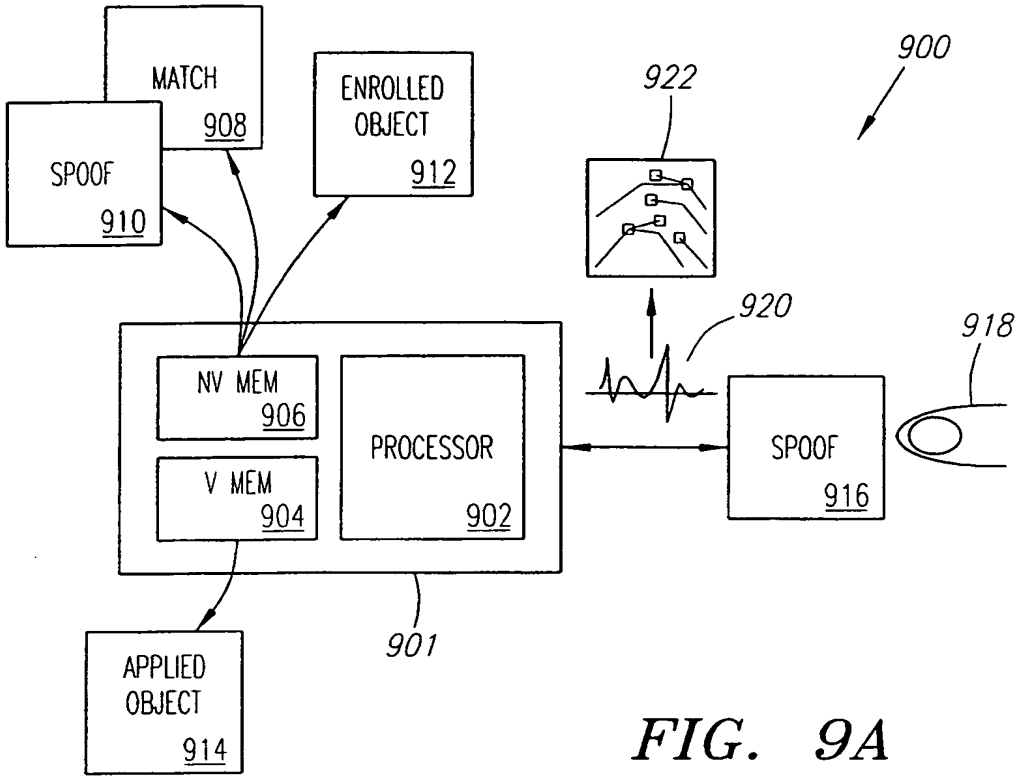


FIG. 9A

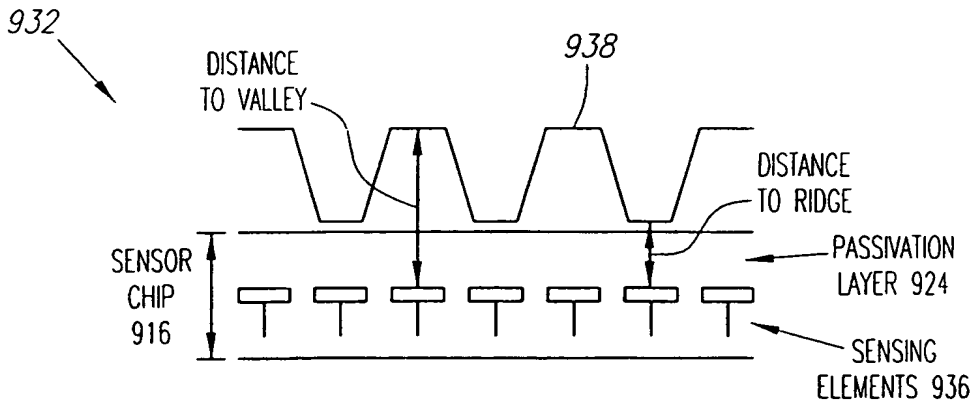


FIG. 9B

BNSDOCID: <WO___0124700A1_I_>

INTERNATIONAL SEARCH REPORT

Inte .tional Application No
PCT/US 00/27782

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 A61B5/117 G07C9/00 G06K9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G07C A61B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 372 748 A (FUJITSU LTD) 13 June 1990 (1990-06-13) abstract ---	1,19,38
X	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 02, 26 February 1999 (1999-02-26) & JP 10 290796 A (NEC CORP), 4 November 1998 (1998-11-04) abstract ---	1,19,38
X	PATENT ABSTRACTS OF JAPAN vol. 015, no. 205 (P-1206), 27 May 1991 (1991-05-27) & JP 03 053385 A (NIPPON DENKI SEKIYURITEI SYST KK), 7 March 1991 (1991-03-07) abstract -----	1,17,19, 35,37,38

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 2001	27/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sonius, M

1

Form PCT/ISA/210 (second sheet) (July 1992)

BNSDOCID: <WO___0124700A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte .ational Application No
PCT/US 00/27782

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0372748 A	13-06-1990	JP 2259969 A	22-10-1990
		JP 2695231 B	24-12-1997
		JP 2307176 A	20-12-1990
		JP 2774313 B	09-07-1998
		JP 2708051 B	04-02-1998
		JP 3087981 A	12-04-1991
		JP 2144685 A	04-06-1990
		CA 2003131 A,C	25-05-1990
		DE 68918244 D	20-10-1994
		DE 68918244 T	02-02-1995
		KR 9302346 B	29-03-1993
		US 5088817 A	18-02-1992
JP 10290796 A	04-11-1998	JP 2962274 B	12-10-1999
JP 03053385 A	07-03-1991	NONE	

BNSDOCID: <WO__0124700A1_I_>

THIS PAGE BLANK (USPTO)

Docket # S&ZIO020405

Applic. #_____

Applicant: ANGELA ENGELS ET AL.

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100 Fax: (954) 925-1101